

"AN IN-DEPTH ANALYSIS OF HUNDREDS OF HIGH-PROFILE AND NEVER-PUBLISHED BEFORE SECURITY RESEARCH ARTICLES AND OSINT ANALYSIS BY THE WINNER OF JESSY H. NEAL AWARD FOR BEST BLOG FOR ZDNET'S ZERO DAY BLOG FOR 2010." - DANCHO DANCHEV

DANCHO DANCHEV'S SECURITY RESEARCH PORTFOLIO FOR ZDNET'S ZERO DAY BLOG

IN-DEPTH OVERVIEW AND ANALYSIS OF
SECURITY BLOGGER DANCHO
DANCHEV'S SECURITY RESEARCH FOR
ZDNET'S ZERO DAY BLOG CIRCA 2008-
2012

BY DANCHO DANCHEV

BBC team buys a botnet, DDoSes security company Prevx | ZDNet

Update: [BBC Click's tweet](#) states that they [took legal advice](#) following comments on the potential [violation of U.K's Computer Misuse Act](#) .

There's a slight chance that you may have unknowingly participated in a recent experiment conducted by the BBC.

In a bit of an awkward and highly unnecessary move, a team at the [BBC's technology program Click has purchased a botnet consisting of 22,000 malware infected PCs](#) , self-spammed themselves on a Gmail account, and later on DDoS-ed a backup site owned by security company Prevx (with prior agreement), all for the sake of proving that botnets in general do what they're supposed to - facilitate cybercrime.

A [video of the experiment](#) is already [available](#) . Here are more details :

Upon finishing the experiment, they claim to have shut down the botnet, and interestingly notified the affected users. Exposing cybercrime or exposing the obvious, [the experiment raises a lot of ethical issues](#) . For instance, how did they manage to contact the owners of the infected hosts given that according to the team they didn't access any personal information on them?

It appears that they [modified the desktop wallpapers of all the infected hosts](#) to include a link notifying them that they've been part of the experiment. Thanks, but no thanks.

Let's talk money, and how much did they pay to get access to the botnet. Despite the fact that they're not mentioning the exact amount, a quote within their article once again puts the spotlight on the dynamics of cybercrime economy :

"Computers from the US and the UK go for about \$350 to \$400 (£254-£290) for 1,000 because they've got much more financial

details, like online banking passwords and credit cards details," he said."

I beg to differ. From my perspective based on the active monitoring of on the growing "botnet for hire" business during the last couple of years, it appears that the BBC got scammed on their way to expose the scammers by overpaying them. In a dynamic underground marketplace where transparency of the sellers and buyers doesn't exist for the sake everyone's anonymity, you are unable to say whether you've made a good or bad deal, since you're unaware of all the propositions. Namely, the botnet you've just purchased is available at a cheaper price from a vendor of whose existence you're not even aware of.

Take a peek at the screenshot from a similar service that's been active for several years, with hosting services provided by "our dear friends" at Layered Technologies, and how cheaper their services are. See, I told you, but I didn't and wouldn't demonstrate you the obvious effectiveness of botnets in general. Take that for granted.

In an interview which I took from [German malware researchers](#) earlier this year, their primary concern for using a methodology that could issue potential disinfection commands to Storm Worm infected hosts was [the legal, and also, ethical side of the practice](#) . Just like the way it should be, since their approach is among the many other the community is taking advantage of on its way to fighting cybercrime.

BBC hit by a DDoS attack | ZDNet

The British Broadcasting Corporation (**bbc.co.uk**) was hit by a DDoS attack on Thursday, according to [a statement sent to the Inquirer](#) :

"In a statement to the INQ, the BBC said the attack originated in a number of different countries but didn't specify which. When the Beeb's techies blocked international access to a limited subset of servers, it resulted in a marked improvement of the serving of bbc.co.uk. Service supplier Siemens was forced to block addresses and prevent the attack using other methods like changing the DNS settings."

The attack appears to have lasted for 1 hour and 15 minutes, which is the longest time the site has been offline during the entire 2008, was also confirmed by the [distributed uptime monitoring company Pingdom](#) earlier today :

"During the attack, the BBC website responded very slowly, and our monitoring shows that for a total of 1 hour and 15 minutes it did not respond at all. The downtime was spread over multiple short intervals, lasting just a few minutes each time. The attack lasted the entire evening. It started to have an effect after 5 p.m. CET and the performance was not back to normal until after 10 p.m. CET. Analyzing the response times of the website clearly shows the effect the DDoS attack had on the performance of the BBC website. The diagram below shows the hourly average load time of the HTML page (just the HTML page, without any images, external scripts, etc)."

Was the attack an act of hacktivism based on a particular article that somehow contradicted with the attackers' perspective of the world? With the lack of specific details regarding the DDoS attack provided by the BBC, we may never know. One thing's for sure - political DDoS attacks ([Georgia President's web site under DDoS attack from Russian hackers](#) ; [Coordinated Russia vs Georgia cyber attack in progress](#)) are going to get even more mainstream in 2009.

What are some of the driving factors contributing to this trend? The overall availability of malware infected hosts, which when once monetized ends up in [DDoS for hire services](#) whose prices for a large scale hourly attack are getting disturbingly affordable to anyone. The recently released "[Worldwide Infrastructure Security Report](#) " report by Arbor Networks also indicates that the [DDoS attack rates exceed the ISP network's growth](#) , and have already reached the 40GB barrier. Ironically, the report also states that managed DDoS mitigation services are increasing, which is exactly what is happening on the DDoS for hire services front - they're becoming ubiquitous as outsourcing DDoS attacks to experienced attackers directly messes up the entry barriers into a space that used to require experience, and an operational botnet a couple of years ago.

Bank of Melbourne Twitter account hacked, spreading phishing links | ZDNet

The Twitter account of Bank of Melbourne was compromised last Wednesday, and was used to spread phishing links as direct messages to the account followers, according to reports coming in from affected users.

In [a tweet](#), the bank said that:

ATTN: Unauthorised DMs sent bw 4-5pm today, do not click link. No customer/personal data compromised. Apologies for the inconvenience. ^TT

Followed by [another one](#), once the incident was resolved:

Thanks for all your support. We take security very seriously & will be strengthening our policies to further protect our social channels ^TT

It's worth discussing how Bank of Melbourne got its social channel hacked in the first place. Moreover, what contributed to the ease of obtaining the login credentials for their Twitter account?

For starters, it would have been highly impractical to brute force the password for their Twitter account, no matter the fact that the [CAPTCHA-solving process could be outsourced to vendors](#) offering CAPTCHA-solving services to assist in brute forcing attacks.

Judging by the fact that the malicious attackers didn't just spread a prank or hacktivist message using the stolen credentials, it is highly likely that the attacker has a relatively advanced understanding of how the cybercrime ecosystem works. By spamvertising the phishing link using direct messages as an evasive element of the campaign, the attacker is attempting to take advantage of the trust factor established by the nature of direct messages.

Was Bank of Melbourne a victim of phishing attack, is there any chance that a malware-infected host within their network was successfully data mined for stolen Twitter credentials.

What do you think?

Talkback.

Baidu DNS records hijacked by Iranian Cyber Army | ZDNet

Earlier today, the DNS records of China's most popular [search engine Baidu](#) were hijacked by a group known as the "[Iranian Cyber Army](#)", and the portal [redirected to](#) a web server featuring a message "*protesting the military intervention of foreign and Israeli sites in our internal affairs division and distribution of false news*".

The DNS hijacking appears to have taken place using the same social engineering elements used in the [DNS hijacking of Twitter.com in December, 2009](#), again orchestrated by [the same hacking group](#).

However, what the "Iranian Cyber Army" wasn't fully aware of, is the fallout of hijacking the DNS records of China's largest search engine - in this case the response of a highly developed collectivist hacking community ([Honker Union For China](#)), which has already started to hack and deface Iranian web sites.

"China's largest search engine, Baidu.com, confirmed Tuesday its website had been temporarily paralyzed after coming under cyber-attack, and an expert on network security warned major websites of domain name server (DNS) protection against hackers. Baidu.com resumed operation at 11:30 a.m. after being down for three and a half hours. The company said later in a statement that Baidu's DNS in the United States was illegally attacked, without giving more information.

Wang Zhantao, an expert with Beijing Rising International Software Co. Ltd., said hackers were increasingly getting used to attacking domain name servers of major websites because they were a chink in cyber security systems. "Many websites like Baidu have almost perfect inner security system, but their DNS security is up to domain name registers," Wang said."

How did the "Iranian Cyber Army" do it? By successfully social engineering the [domain registrar](#), or the [domain registrant](#) in this

case a Baidu employee with access to the control panel, the attackers were able to [direct the traffic to any location of their choice.](#)

The same tactic used in some of the most notable DNS hijackings that took place over the past two years, proving that an old-fashioned attack vector in cases where the attacker cannot compromise the site itself, remains fully working.

Ironically, in June 2009, Twitter which had its DNS records hijacked by the "Iranian Cyber Army", played a key role in helping the Iranian opposition organize a crowdsourcing DDoS ([Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites](#)), which managed to shut down key government web sites without the reliance on any botnet.

Go through related DNS hijacking incidents: [Comcast's DNS records hijacked, redirect to hacked page \(2008\)](#) ; [How was Comcast.net hijacked? \(2008\)](#) ; [Photobucket's DNS records hijacked by Turkish hacking group \(2008\)](#) ; [ICANN and IANA's domains hijacked by Turkish hacking group \(2009\)](#) ; [Hackers hijack DNS records of high profile New Zealand sites \(2009\)](#)

The response from a well known Chinese hacktivist group, the Honker Union of China, came shortly with an ongoing campaign to hack and deface Iranian web sites in order to "*let the world hear the voice of China* " and "*defend the country's dignity across the world* ".

Just like we've already seen the tactic used in 2008's "[Coordinated Russia vs Georgia cyber attack in progress](#) ", the Chinese hacktivists are already distributing a list consisting of high-profile Iran government web sites as a potential targets.

[Next](#) -->

The exact messages found on six currently defaced web sites (**ksh-behzisty.gov .ir** ; **iribu .ir** ; **diabetes .ir** ; **room98 .ir** ; **irun .ir** ; **behdasht.gov .ir**) :

I'm very sorry for this Testing! Because of this morning your Iranian Cyber Army Maybe you haven't konw this thing! This morning your Iranian Cyber Army intrusion our baidu.com So i'm very unfortunate for you Please tell your so-called Iranian Cyber Army Don't intrusion chinese website about The United States authorities

to intervene the internal affairs of Iran's response This is a warning!
Khack by toutian...from...Honker Union For China

Rini Ma Iranian chicken child, the small A coming, Iranian chicken child, your mother in Iraq for a P, go back to Iraq, your mother, he committed me, "Baidu," I f*** you mother QQ409882525

{We are Chinese hackers} {Chinese people are hacking} {The Chinese are a bad bully, small JB Iran}

Related screenshots from the defaced sites in response to the DNS hijacking of Baidu.com:

The DNS hijacking [affected the site for a period of three and a half hours](#) , which according to Xinhua news agency results in the longest downtime period since December 2006.

Interestingly, several questions remain unanswered. For instance, just because a hacking group describes itself as the "Iranian Cyber Army", writes in Farsi and leaves propaganda messages, does it automatically mean that the group is indeed of Iranian origin?

And even if it is, [how long before the world starts taking seriously a group describing itself as](#) "North Korea's Cyber Army", as a government-funded hacking team, the implications of which could be pretty serious on an international level?

What do you think? Talkback.

Bad, bad, cybercrime-friendly ISPs! | ZDNet

In a [post-McColo](#) , [post-Atrivo](#) and [post-EstDomains](#) cybercrime [ecosystem](#) , the researchers at [FireEye](#) have recently launched a "Bad Actors series" aiming to put the spotlight on some of the currently active badware actors online. The sampled ISPs represent safe heavens for drop zones for banker malware, DNSChanger malware, rogue security software and live exploit URLs.

From [Starline Web Services](#) , to [ZIKon](#) , [Internet Path/Cernel](#) , [HostFresh](#) and [UralNet](#) , the series draw a simple conclusion - that a dysfunctional abuse departments can indeed act as driving factor for the growth of cybercrime.

The main objective of a dysfunctional abuse department is to on purposely delay the review and take down process of a domain/customer in question, thereby increasing the average time for the campaign to remain online. Which is exactly what most of these ISPs are involved into, while charging premium prices in the process of ignoring community requests for shutting down a malicious campaign in question.

Interestingly, what we're witnessing for the time being is a mixed abuse of, both, legitimate infrastructure and purely malicious one. For instance, the bad actors that FireEye is profiling, will receive traffic coming from abused legitimate infrastructure such as the [Digg](#) , [Google Video](#) and [YouTube's](#) latest malware campaigns. Moreover, we cannot talk about cybercrime-friendly ISPs without mentioning the [domain registrars of choice for the majority of cybercriminals](#) , which KnuiOn keeps profiling. Their February, 2009 Registrar Report states that 10 registrars are responsible for 83% of the fraudulent sites that they've analyzed, with the Chinese registrar **XIN NET** topping the chart for a second time.

With new cybercrime-friendly ISPs popping up on the radar, consider keeping an eye on the upcoming additions to [the bad actors series](#) .

Image courtesy of [Google's Postini 2008 Spam Report](#) in a post-McColo Internet.

AVG and Rising signatures update detects Windows files as malware | ZDNet

Yesterday, [a signatures update pushed by AVG](#) falsely labeled a critical Windows file as a banker malware, prompting the company to quickly fix the issue and issue a workaround, following end users complaints at its support forums.

AVG's false positive causing downtime for Windows users is happening a week after [Rising antivirus apologized to its customers](#) for falsely detecting [Outlook Express as malware](#) leading to loss of emails, and yes, productivity too.

The [impact of the false positive](#) leads to a continuous reboot cycle :

"An update for the AVG virus scanner released yesterday [contained an incorrect virus signature](#) , which led it to think user32.dll contained the Trojan Horses PSW.Banker4.APSA or Generic9TBN. AVG then *recommended deleting this file* ; this causes the affected systems to either stop booting or go into a continuous reboot cycle. So far, the problem only appears to affect Windows XP, but there is no guarantee that other versions of Windows don't have the same issue."

[AVG's brief response](#) to the situation, with the workaround posted at [AVG's support section](#) under the "False positive user32.dll" title :

"Unfortunately, the previous virus database might have detected the mentioned virus on legitimate files. We can confirm that it was a false alarm. We have immediately released a new virus update (270.9.0/1778) that removes the false positive detection on this file. Please update your AVG and check your files again.

We are sorry for the inconvenience and thank you for your help.

Best regards, Zbynek Paulen AVG Technical Support"

AVG and Rising aren't an exception to previous cases where components of Microsoft's Windows have been detected as false

positives. In fact, in 2006 Microsoft's Anti-Spyware was detecting a competing solution as a piece of malware :

[CA's eTrust false positive for a Windows component](#) - **2006**
[Microsoft Anti-Spyware false positive for Norton Antivirus](#) - **2006**
[Kaspersky's false positive of Windows Explorer](#) - **2007** [Symantec's false positive of Windows XP](#) - **2007** [Trend Micro's false positive for Windows](#) - **2008**

Response time is crucial in such a situation, so the best thing the vendors can do is go public and provide assistance in fixing the problem.

AutoRun malware infections declining | ZDNet

Following [February's update issued by Microsoft](#) limiting the propagation of AutoRun-based malware on Windows XP, the company has just reported that the move is working and that [Microsoft is observing a significant decline in the propagation of AutoRun-based malware](#).

More specifically, the company is observing a 59% decline on XP, followed by 74% on Vista in comparison to the 2010 infection rates:

62 percent decrease on Windows XP SP 3

68 percent decrease on Windows Vista SP 1

82 percent decrease on Windows Vista SP 2

Millions of users continue using pirated Windows copies, preventing them from obtaining the latest Windows Updates, thereby exposing themselves to malware attacks.

Why do you think users continue using pirated copies of Microsoft's products, thereby exposing themselves to security risks? [Does software piracy really lead to higher malware infection rates?](#)

What do you think?

Talkback.

Attacks on NFC mobile phones demonstrated | ZDNet

Yesterday, Collin Mulliner of the [trifinite.group](#) , a group of computer experts researching insecurities in wireless

communications, has released [the slides](#) as well as the [research tools](#) he came up with in order to demonstrate various attacks and vulnerabilities in [Near Field Communication](#) mobile phones, a technology that will change the face of [mobile payments](#) , and naturally result in more innovative mobile phishing and malware attempts. A summary of his research presented at [last week's EUSecWest](#) :

Near Field Communication (NFC) based services and mobile phones are starting to appear in the field, therefore it is time to take a look at the security of the services and especially the NFC mobile phones them self's. The presentation will provide this first look at the security of NFC mobile phones. We will show some known theoretical attacks and how they may work in the field. Further we will present results from analyzing a specific NFC mobile phone, here we will reveal some security issues and methods to exploit them. Also we will provide a small survey of NFC applications in the field. Finally we will release a small set of tools to do further analysis on NFC mobile phones and applications.

We recognize that NFC is not widely used yet but we anticipate that it will be in the near future due to the massive effort carried out by the member companies (http://www.nfc-forum.org/member_companies/). Also since NFC is based on RFID technology (ISO 14443) the whole topic should be highly interesting for wide range of security professionals and researchers. The innovative part of this presentation is that it is the first presentation on this topic and it shows mainly real world attacks and provides some hands-on experience for the security people and application developers.

The attacks demonstrated are trivial due to the manufacturer time to market (TTM) obsession, thereby shipping devices with trivial vulnerabilities, in Mulliner's research they orbit around passive tags which are mostly abused as vectors for the any of the attacks demonstrated. What about the market's acceptance of the technology?

Mastercard has just announced that it's starting [a mobile contactless payment pilot across Canada](#) , citing interesting survey results that a malware author or a phisher would definitely enjoy :

Interest in it isn't raging yet, according to IDC Canada's vice-president of communications and segments Tony Olvet. He cited a 2007 survey of 541 15-to-29-year-olds, where 8.8 per cent of them said they would be interested in contactless payments via cell phone. He said that, once visibility of these technologies increases with the PayPass and PayWave trials and rollout, interest will most likely rise.

Let interest rise proportionally with the shipped pre-audited devices, where security and awareness on the potential threats isn't sacrificed for achieving your TTM objective.

Attacker: Hacking Sarah Palin's email was easy | ZDNet

A college student identified as [Rubico](#) has [claimed responsibility for hacking into Sarah Palin's personal email](#) , and provided a detailed 1st person account of how he hacked into the email account using the password "popcorn" which he managed to reset by successfully answering her security question "Where did you meet your spouse?" by Googling for the answer :

"Hello, /b/ as many of you might already know, last night sarah palin's yahoo was "hacked" and caps were posted on /b/, i am the lurker who did it, and i would like to tell the story. In the past couple days news had come to light about palin using a yahoo mail account, it was in news stories and such, a thread was started full of newfags trying to do something that would not get this off the ground, for the next 2 hours the acct was locked from password recovery presumably from all this bullshit spamming.

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!) the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs. I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower."

Originally [blamed for the email hijacking](#) , the Anonymous [movement against the Church of Scientology](#) has distanced from the hack :

"One of the main tenets of the anonymous movement against the Church of Scientology is to stay legal. Anonymous is no fixed group, just a term for anyone who acts without giving their name. We don't know who is responsible for the hack on Sarah Palin's mail account or what their attitudes to Scientology or anything else are. For us, they are anonymous, because we don't know who they are and they are not us."

Meanwhile, the [owner of the Ctunnel.com service recently commented](#) that if the attacker's screenshot didn't include the

complete URI using Ctunnel.com it would have been hard to track him down through his service since a lot of people login to their Yahoo mailboxes while using it. And since the attacker did include the complete URL, and [according to him did a mistake by using a single proxy service](#) next to taking advantage of "proxy chaining" by using multiple different proxy servers/services across the globe, [the FBI has already approached the owner of Ctunnel.com](#) .

It's also worth pointing out that in the time of posting this, Wikileaks.org's article on "[Sarah Palin Yahoo account 2008](#) " has been defaced with the following message, reminding us that Wikileaks has a "fan club" too :

"I NOW HACK THIS WEBSITE! AREN'T YOUR PROUD OF ME, WIKILEAKS. I CAN PLAY YOUR GAME TOO!!!"

The massive media coverage is covering nothing else but an old school password reset tactic made possible due to the oversupply of personal information regarding the victim. Moreover, this incident once again puts the "security question vulnerability" in the spotlight. Last month, [a posting at SecuriTeam's blogs](#) reasonably pointed out how personalizing the security question to something a little less obvious, is a feature currently offered only by Gmail, which shouldn't be the case despite the fact that anyone can give an entirely different answer to each of the common "security" questions asked :

"Anyone that knows my address can easily figure out the name of my first school or my high school mascot. All of my neighbors, family and friends know both my dog's name and my dad's middle name, and everybody in the world knows I just LOVE the Lakers. As for my wife and me, the people who attended our wedding had the chance

to hear about it in the ceremony - in case you couldn't make it, we met on a roof of a bus, in Ladakh, India in 1994...

The fact that the answer to each of the security questions above is relatively easy to find out, makes them a security vulnerability in my Yahoo! account. By letting me make a security key based on the name of my first school, Yahoo! actually puts me at risk, allowing anyone that knows where I live to hijack my account. It's like saying "We have the greatest lock to protect your house. Now, why don't we hide the key under the mat".

Hacking is supposed to be about intellectual exploration, so resetting the password of someone's Yahoo mailbox no matter if it's the Pope, requires no more than two brain cells put into action. However, the political consequences and the long-term impact of this hack are an entirely different topic yet to be discussed based on the interpretation of the data found within.

Attack of the Opt-In Botnets | ZDNet

What's more devastating than a DDoS attack launched by a botnet? In some cases, that's the DDoS attack launched by the "opt-in botnet" aggregated through a crowdsourcing campaign.

Damballa's recently released report "[The Opt-in Botnet Generation: Social Networks, Cyber Attacks, Hacktivism and Centrally-Controlled Protesting](#)" describes the increasing sophistication of cyber-protesting tools, for launching political protests around the globe.

Let's review seven well known and extensively profiled examples of "opt-in botnets" and crowdsourcing campaigns, to find out why some failed and others succeeded.

What exactly is an opt-in botnet? What are some of the most notable cases where it has been successfully used? How can you disrupt a opt-in botnet given that the command and control server is in the hands of every user knowingly participating in it?

Damballa's report describes "opt-in botnets" as:

"In practically all criminal botnet cases in the past, the owners or users of the bot-infected computers have been unwitting participants in an attack. This aspect of botnet participation fundamentally changes in the context of cyber-protesting, since as users intentionally install botnet software agents, subscribe to a particular CnC, and choose to participate in coordinated attacks against a target category. Whether it's because of a vagueness in the understanding of laws governing cyber attacks and electronic denial of service, or a perception of only being a small cog in a much wider effort that will never result in them being singled out, there seems to be few inhibitors to taking protesting in to the cyber world and taking an active role in the call to action."

Just like real botnets, opt-in botnets need a command and control server from where to issue new commands, and accept status reports on the success/failure of the DDoS attack.

What's particularly interesting about opt-in botnets is their reliance on popular social networks such as Facebook, or micro-blogging services like Twitter, both acting as the command and control center for scheduling the attack, and distributing the attack tools.

"Three Twitter accounts, five Yahoo! Mail accounts, twelve Google Groups, eight Blogspot blogs, nine Baidu blogs, one Google Sites and sixteen blogs on blog.com that we being used as part of the attacker's infrastructure " - [Researchers expose complex cyber espionage network](#)

And whereas the use of legitimate networks as "virtual human shields" against potential take efforts ([Twitter](#) , [Google Groups](#) , [Amazon's EC2](#) , [Facebook as command and control servers](#)) is nothing new, given the millions of active users and the increase ease of reaching the citizens of a particular country only, a well organized campaign could achieve its objectives by nothing else besides setting up a Facebook group, or promoting a Twitter hashtag.

Just how successful is the concept of "opt-in botnets", also known as "people's information warfare" or the "malicious culture of participation? Let's review some of the well known campaigns that relied on "opt-in botnets", and crowdsourcing tactics to achieve the DDoS effect.

[Examples of Opt-in Botnets/Crowdsourcing](#) -->

- [Make Love Not Spam opt-in botnet campaign](#) - 2004

The campaign claims to have attracted over 110,000 participants who installed their [screensaver launching DDoS attacks at over 100,000 spam sites](#) :

"Lycos Europe's approach has been cheered by some Internet users fed up with spammers' abuse of their mailbox and connectivity. The UK-based firm appears to be relying on the likelihood that the renegade sites being targeted are unlikely to use legitimate channels (such as ISP abuse departments) to report attackers. No Internet service providers have yet indicated that they will take action against subscribers participating in the attacks. "

The opt-in botnet was introduced, surprisingly, by [Lycos Europe who shut down the campaign on December 21, 2004](#) due to

criticism.

- [The failed Electronic Jihad \(e-jihad.exe\) crowdsourcing attempt - 2007](#)

In November, 2007, a [cyber jihadist site know as Al-Jinan](#) started publicly coordinating a DDoS attack against Western sites. And whereas [the target list](#) later on included anything else but Western sites, the campaign was a complete failure for its organizers.

How come? Not only was their central coordination point, the official site in question shut down, but also, they have embedded a single phone back location for the application to connect back and obtain the list of the targets. Again, that was the central coordination site.

- [The successful DDoS attack against CNN.com courtesy of Chinese hacktivists -2008](#)

[Next to the DDoS attack against CNN.com](#), this crowdsourcing attempt was perhaps among the first to utilize multiple attack tactics such as web site defacements resulting in the compromise of CNN sports to spread Pro-Chinese messages against Tibet.

Was the campaign successful? [According to NetCraft](#) :

"The CNN News website has twice been affected since an earlier distributed denial of service attack last Thursday. CNN fixed Thursday's attack by limiting the number of users who could access the site from specific geographical areas. Subsequently, an attack was purportedly organised to start on Saturday 19th April, but canceled.

However, our performance monitoring graph shows CNN's website suffered downtime within a 3 hour period on Sunday morning, followed by other anomalous activity on Monday morning, where response times were greatly inflated. Netcraft is continuing to monitor the CNN News website. Live uptime graphs can be viewed [here](#). "

- [The Russia vs Georgia cyber attack, a combination of crowdsourcing and standard botnet - 2008](#)

Next to the [2009's cyber attack against Pro-Ahmadinejad sites](#) , this campaign is a personal case study on the sophisticated understanding of the basics of cyber operations shown on behalf of the Russian attackers.

What's so impressive about their tactics? It's the convergence of PSYSOPS (psychological operations) standardized web site defacements spreading identical messages, a clear planning phrase based on the publicly distributed lists of Georgian sites susceptible to SQL injection attacks, a self-mobilization on behalf of Russian cybercriminals, and the crowdsourcing element in the face of thousands of Russians attacking Georgian sites.

Moreover, the Russian campaigners also took offline one of Georgia's most vibrant hacking forums offline in an attempt to prevent Georgian hacktivists to organize themselves.

[More examples of Opt-in Botnets/Crowdsourcing](#) -->

- [The crowdsourcing cyber attack against Pro-Ahmadinejad sites - 2009](#)

What this campaign demonstrated was literally everything [Damballa is discussing in their report](#) .

Excessive coordination took place through Twitter, in between the countless number of separate coordination sites, followed by a systematic supply of fresh proxy IPs given the censorship efforts aimed at social networking sites at the time of the attacks.

What's particularly interesting to point out about the campaign was the paradox of the ["self-eating" Internet infrastructure of Iran](#) :

"Moreover, the majority of people's information warfare driven cyber attacks we've seen during the past two years, have all been orbiting around the scenario where a foreign adversary is attacking your infrastructure from all over the world. But in the current situation, it's Iran's internal network that's self-eating itself, where the trade off for denying all the traffic would be the traffic which could be potentially influenced through PSYOPs (psychological operations). "

The scale of the campaign was in fact so massive, that calls to stop attacking government sites and news agencies were made in

order to allow Iranian people to use the Internet as a distribution channel for user-generated content streaming from the country.

This disagreement over whether DDoS-ing is better than contributing user-generated content, eventually resulted in the overall decline of the DDoS efforts.

- The Pro-Israeli crowdsourcing DDoS attempt - 2009

Failed attempt organized by the "Help-Israel-Win movement" in an attempt to entice users into joining an "opt-in botnet" targeting pro-Hamas web sites.

"We created a project that unites the computer capabilities of many people around the world. Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel. The more support we get, the efficient we are! You download and install the file from our site. The file is harmless to your computer and could be immediately removed. There is no need for identification of any kind - anonymity guaranteed! "

This campaign is an example of a badly executed one, with zero utilization of social media, with contributed to the quick demise of its central redirection point, and the small number of people that downloaded their software and became part of it.

- 'Anonymous' group's DDoS attempt against the Australian government - 2009

Another failed crowdsourcing attempt -- in comparison their **most recent attack in February, 2010** was successful -- due to the campaign's lack of social media promotion and interaction with potential users who could have opted-in.

Although the group is clearly familiar with IRC (Internet Relay Chat), Generation Y isn't, and doesn't want to.

"Operation Didgeridie consists of the distribution of DIY denial of service attack tools ([404ServerNotFound.exe](#)), launching "Fax bombs" using a [GetUp! Campaign script](#) , enticing into direct server compromise attempts by distributing a recently performed [web application vulnerability assessment](#) of Australian government web site using commercial tool. "

Damballa's "[The Opt-in Botnet Generation: Social Networks, Cyber Attacks, Hacktivism and Centrally-Controlled Protesting](#)," concludes that the threats will only grow in scale and seriousness due to the ease of establishing these botnets and the ever-increasing penetration of social networks in our daily lives.

A good question emerges from the report's conclusion - how thin is the line between being the victim, and being the enabler?

In the event of crowdsourcing driven cyber attack, would you "surrender" your bandwidth?

TalkBack.

Atrivo/Intercage's disconnection briefly disrupts spam levels | ZDNet

After years of operation, California based ISP Atrivo/Intercage, a well known Russian Business Network darling, faced the music and was disconnected from the Internet [by its upstream provider at the end of September](#) . What happened [according to MessageLabs's latest intelligence report](#) , was a brief decline of spam due to the fact that the malware infected hosts couldn't reach the ISP's netblock. Logically, within the next couple of days Intercage's customers quickly switched hosting locations of their botnet's command and control servers, and cybercrime activity quickly got back to normal :

"Charged with providing a safe-haven for online scammers, cyber crooks and malware distributors, California-based ISP Intercage (aka Atrivo) was disconnected from the internet on September 20. Pacific Internet Exchange, Intercage's upstream provider, terminated the service and after a few days, UnitedLayer, another service provider, agreed to host Intercage. But on September 25, after deciding Intercage still had too many on-going problems, UnitedLayer also terminated service.

It can be seen from the chart above that the botnet controllers are quick to respond to any degradation of their service, and can re-point their bots at a new command and control channel in a matter of days. Therefore MessageLabs expects this decline in spam to be short-lived, especially in anticipation of Halloween in October and Thanksgiving in the US in November, both of which are traditionally seasonal favorites for spammers."

What's particularly disturbing in Intercage's case is not just the fact that it's a U.S based ISP undermining the "lack of international cybercrime cooperation" excuse for not shutting it down earlier, but also, the fact that ATRIVO/Intercage's uptime is a great example of how marginal thinking and relatively high average time it takes to shut them down, is nonetheless still keeping their business in the game. How come? [For the past year, ATRIVO/Intercage has had 10](#)

[different Internet Service Providers](#) , so controversially to the common wisdom that being on the run is supposed to make your job harder, it doesn't really matters as the average time for ATRIVO to remain online seems to be above their customers' averages :

"The following graph shows that Atrivo has had 10 different Internet providers over the past year. The number of Renesys peers selecting each provider is shown over time. Most providers didn't stick around for long, but a few like WV Fiber (AS 19151) did hang in there for much of the year. For a couple of days recently, Atrivo had zero providers and were hence effectively out of business, but then United Layer (AS 23342) became their latest — and currently only — provider. We'll see how long this lasts and if others step up to provide Atrivo with some redundancy. Of course, those who are convinced Atrivo is up to no good can simply block access to their IP addresses (prefixes) as they have a relatively modest allocation."

Do bullet-proof cybercrime friendly providers have a future? Naturally, since it's the simple market forces that are going to keep both fronts busy for years to come. With ATRIVO/Intercage now shut down, what's next? Lessons learnt for the bad guys realizing that it's about time they start taking advantage of [basic OPSEC \(operational security\)_processes](#) like decentralizing their networks, and [increasing the lifecycle of their customer's cybercrime activities](#) by taking advantage of fast-fluxing. The bottom line, despite that Intercage remains offline, but the concepts of cybercrime content hosting, and [the Russian Business Network as a franchise](#) , are always going to be there.

Asus ships Eee Box PCs with malware | ZDNet

Asus has confirmed and apologized to customers ([press release](#) in Japanese; [translated version](#)) for shipping malware on the recently introduced [Eee Box desktop computer](#) :

"According to an email sent out by Asus, PC Advisor reports, the Eee Box's 80GB hard drive has the recycled.exe virus files hidden in the drive's D: partition. When the drive is opened, the virus activates and attempts to infect the C: drive and any removable drives connected to the system. According to Symantec, the malware is likely to be the [W32/Usbalex worm](#) , which creates an autorun.inf file to trigger recycled.exe from D:. Separately, we've been testing the Eee Box this week, and discovered our review unit came loaded with the W32/Taterf worm - aka [W32.Gammima.AG](#) , aka kavo.exe malware that sniffs out online gaming usernames and passwords.

Which models are known to carry the malware according to Asus?

The company has already managed to identify the following models with associated UPC codes :

Model number: EEEBOXB202-B; **UPC code:** 610839761807
Model number: EEEBOXB202-W; **UPC code:** 610839761814
Model number: EBXB202BLK/VW161D; **UPC code:** 610839530526
Model number: EBXB202WHT/VW161D-W; **UPC code:** 610839531202
Model number: EBXB202BLK/VK191T; **UPC code:** 610839547753

In addition to [last month's Asus fiasco](#) when they accidentally shipped cracking tools and confidential documents on recovery DVDs, the company is among the increasing number of companies that have shipped malware on their products during the last couple of years - [Apple](#) (2006), [TomTom](#) (2007), [Seagate](#) (2007), and [HP](#) (2008).

Ashton Kutcher's Twitter account hacked | ZDNet

The Twitter account of Ashton Kutcher appears to have been compromised over the past 24 hours, based on two tweets posted on behalf of him.

[First tweet](#) :

Ashton, you've been Punk'd. This account is not secure. Dude, where's my SSL?

[Second tweet](#) :

P.S. This is for those young protesters around the world who deserve not to have their Facebook & Twitter accounts hacked like this. #SSL

Although the [SSL sniffing which theoretically can take place](#) is clearly not malicious in this case, the potential for abuse -- malware, scams, phishing links -- given Kutcher's 6 million followers, remains a fully realistic scenario if it was.

Approximately 800 vulnerabilities discovered in antivirus products | ZDNet

UPDATE: [McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position](#) . In what appears to be either a common scenario of "when the security solution ends up the security problem itself", or a

product launch basing its strategy on outlining the increasing number of critical vulnerabilities found in competing antivirus products, the [IT/Security consulting firm n.runs AG](#) claims to have [discovered approximately 800 vulnerabilities within antivirus products](#) based on exploiting a standard malware scanning process known as "parsing" :

"During the past few months, specialists from the n.runs AG, along with other security experts, have discovered approximately 800 vulnerabilities in anti-virus products. The conclusion: contrary to their actual function, the products open the door to attackers, enable them to penetrate company networks and infect them with destructive code. The positioning of anti-virus software in central areas of the company now poses an accordingly high security risk. The tests performed by the consulting company and solutions developer n.runs have indicated that every virus scanner currently on the market immediately revealed up to several highly critical vulnerabilities. These then pave the way for Denial of Service (DoS) attacks and enable the infiltration of destructive code – past the security solution into the network. With that, anti-virus solutions actually allow the very thing they should instead prevent."

In between the ongoing efforts put by malware authors to obfuscate their binaries, release as many as possible in the shortest time frame achievable, or ensure that they bypass the most popular personal firewalls before releasing them by [applying quality assurance to their malware campaigns](#) , can antivirus products be a security issue themselves? But of course, and the increasing number

of vulnerabilities discovered is clearly indicating the increasing interest in proving the point in general.

[How did n.runs manage to discover the vulnerabilities they claim they found?](#) By following the very same logic on which a great deal of the

current vulnerabilities are based on, the way in which the scanner parses the file it's supposed to scan :

"In this context, n.runs was able to make out so-called "parsing" as one of the main causes of this boomerang effect. The principle functions as follows: virus scanners must recognise as many "Malware" applications as possible – and thereby comprehend and process a large number of file formats. In order to be able to interpret the formats, an application must partition the corresponding file into blocks and structures. This separation of data into analysable individual parts is called "parsing". Mistaken assumptions in the course of programming the parsing code create constellations which enable the infiltration and subsequent running of programme code. Moreover, the quick reactions time expected by developers (regarding threats) contributes to a decrease in the quality of the code. In short: the more parsing that takes place, the higher the recognition rate and the degree of protection from destructive software, but at the same time, the larger the attack surface – which makes the anti-virus solution itself a target."

The research they cite is based on [Secunia's](#) tracking of advisories affecting antivirus products, as well as research conducted by the University of Michigan emphasizing on the severity of the vulnerabilities on a per product basis. For instance, between 2002 and 2005 there were 50 advisories regarding vulnerabilities affecting antivirus products, but between 2005 and 2007, there's been an increase of 240% with 170 advisories. Moreover, according to a research paper by Feng Xue, presented at this year's Blackhat Europe, according to the U.S national vulnerability database, [165 vulnerabilities within antivirus products](#) have been reported during the last 4 years. It's even more ironic to point out that the now fixed [remote code execution vulnerability in Panda Security's online virus](#)

[scanner](#) , further proves that the security solution can indeed end up the security problem itself.

With the increasing interest and success into finding critical security vulnerabilities within antivirus products, are we going to see more abuse of these "windows of opportunity" by malware authors themselves? I don't think so, at least not on a large scale. What they are going to continue researching are ways in which to [shut down the antivirus solution silently](#) , prevent it from reaching its hard coded update locations, and most importantly ensure the malware has been [pre-tested against the most popular security solutions](#) before it's released in the wild - precisely what they've been doing for the last couple of years.

Apple releases QuickTime 7.7.3 for Windows, patches critical security vulnerabilities | ZDNet

Apple just released [QuickTime 7.7.3 for Windows](#), patching critical security vulnerabilities that could allow arbitrary code execution.

More details on the patched vulnerabilities:

[CVE-2011-1374](#) - Viewing a maliciously crafted PICT file may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3757](#) - Viewing a maliciously crafted PICT file may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3751](#) - Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3758](#) - Viewing a maliciously crafted QuickTime TeXML file may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3752](#) - Viewing a maliciously crafted QuickTime TeXML file may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3753](#) - Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3754](#) - Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3755](#) - Viewing a maliciously crafted Targa file may lead to an unexpected application termination or arbitrary code execution

[CVE-2012-3756](#) - Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution

Users are advised to [upgrade to the latest version](#) immediately.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Antivirus vendor introducing virtual keyboard for secure Ebanking | ZDNet

Kaspersky's most recent product launch of the [Kaspersky Internet Security 2009](#) , is featuring a virtual keyboard "a secure pop-up that enables logins, passwords, bank card details and other important personal information to be entered safely to prevent the theft of confidential information " aiming to protect users from keyloggers, and consequently provide a safer Ebanking experience. [More info](#) :

"Full details have yet to be confirmed, but it is understood that the program will let users bring up the keyboard from which to enter login details for Web sites such as online banks that might be vulnerable. The on-screen keyboard will cache the keystrokes, protecting them from recording programs that would pick up physical keystrokes coming via the keyboard driver. It's not a new idea but Kaspersky is the first major security vendor to include such a feature in a standard Net security program. "

Would keylogging evolve into clicklogging? Truth is, clicklogging courtesy of a malware has been around since 2006.

Going mainstream with such a feature, means the vendor has built enough confidence in its ability to provide a safer Ebanking experience. However, it doesn't, at least not in its current form, and in respect to the current threatscape that has long forgotten what keylogging is, perhaps due to the two-factor authentication used, so that every decent [banker malware](#) out there is [taking advantage of form](#) , session, and [TAN grabbing](#) rendering SSL and two-factor authentication irrelevant.

Back in 2006, prior to [an analysis released by Hispasec](#) (the folks behind Virustotal.com) regarding a banker malware that was [successfully defeating virtual keyboards](#) , I made a comment that's [still relevant two years later](#) as far as virtual keyboards are concerned :

"Anything you type can be keylogged, but generating videos of possibly hundreds of infected users would have a negative effect on

the malware author's productivity, which is good at least for now. Follow my thoughts, the majority of virtual keyboards have static window names, static positions, and the mouse tend to move over X and Y co-ordinates, therefore doing a little research on the most targeted bank sites would come up with a pattern, pattern that should be randomized as much as possible. Trouble is, the majority of phishing attacks are still using the static image locations of the banks themselves, when this should have long been randomized as well. OPIE authentication, suspicious activity based on geotagging anomalies, and transparent process for the customer -- please disturb me with an sms everytime money go out -- remain underdeveloped for the time being."

A year later, [proof of concept on defeating Citibank's virtual keyboard](#) was released online that worked even though Citibank's virtual keyboard was [displaying the keys in a random position](#) in a virtual keyboard. [Ebanking malware](#) is anything but old-fashioned, and so instead of coming up with features that the developers behind the most popular crimeware kits think would work in a real life situation, they've started developing specific modules based on the authentication and sessions of the most popular banks on a per country basis.

It would be very interesting to monitor the developments on the keylogging front, especially now that an antivirus vendor is going mainstream with the feature, meaning it would attract a lot of malicious attention for sure, since users would be logging in using it at many other places next to their bank accounts.

Anti fraud site hit by a DDoS attack | ZDNet

The popular British anti-fraud site **Bobbear.co.uk** is currently under a DDoS attack (distributed denial of service attack) , originally launched last Wednesday, and is continuing to hit the site with 3/4 million hits daily from hundreds of thousands of malware infected hosts mostly based in Asia and Eastern Europe, according to the site's owner. Targeted DDoS attacks against anti-fraud and volunteer [cybercrime fighting communities](#) clearly indicate the impact these communities have on the revenue stream of scammers, and with Bobbear attracting such a high profile underground attention, the site is indeed doing a very good job.

Anyway, who's behind this attack? Let's track down a well known DDoS for hire provider currently operating [10 Black Energy DDoS botnets](#) , and take an exclusive peek at his switchboard indicating that 4 of his botnets are currently set to attack **Bobbear.co.uk** only, proving that the attack may have well been outsourced. With [cybercriminals so overconfident](#) in their abilities to remain unnoticed so that they're using a well known botnet command and control server historically used to manage Zeus banker malware campaigns, it's fairly easy to connects the dots :

"Bob Harrison, the administrator of the Bobbear website, got in touch with me this weekend to tell me that his site was under fire from a distributed denial-of-service (DDoS) attack using compromised botnet computers around the world. The botnet is bombarding Bob's website with traffic, effectively blasting it off the internet and making it impossible for legitimate visitors to reach the site.

Moreover, as you can see in this exclusive screenshot attached, 4 of their botnets are currently set to attack **Bobbear.co.uk** using the following preferences :

```
"icmp_freq = 10 icmp_size = 2000 syn_freq = 10 spoof_ip= 0
attack_mode = 0 max_sessions = 30 http_freq = 50 http_threads = 4
tcpudp_freq = 20 udp_size = 1000 tcp_size = 2000 cmd = flood http
bobbear.co.uk ufreq = 5 botid = (not set)"
```

The **Bobbear.co.uk** DDoS attack is only the tip of the iceberg, as while tracking down the source of the attack I've also managed to establish a direct connection between his DDoS for hire services and the [DDoS attacks against the Georgian government](#) , once again proving that DDoS and cybcrime in general is getting easier to outsource these days.

Anonymous leaks 90,000+ emails from compromised military contractor Booz Allen Hamilton | ZDNet

According to a recently published torrent file, the latest victim of the Anonymous movement is the military contractor Booz Allen Hamilton. Hacktivists from the movement have published over 90,000 military emails and password hashes belonging to military and government representatives:

We infiltrated a server on their network that basically had no security measures in place. We were able to run our own application, which turned out to be a shell and began plundering some booty. Most shiny is probably a list of roughly 90,000 military emails and password hashes (md5, non-salted of course!).

We also added the complete sqldump, compressed ~50mb, for a good measure. We also were able to access their svn, grabbing 4gb of source code. But this was deemed insignificant and a waste of valuable space, so we merely grabbed it, and wiped it from their system. Additionally we found some related data on different servers we got access to after finding credentials in the Booz Allen System. We added anything which could be interesting.

Anonymous have also included a penetration testing invoice in the torrent's release notes, emphasizing on the security practices applied to the hacked network.

Although the leak is embarrassing for Booz Allen Hamilton, the post-hack effect could easily set up the foundations for successful spear phishing attacks targeting unpublished U.S military and government emails.

The Anonymous community is thriving. Who's next on their targets list?

TalkBack.

Anonymous launches 'Operation Global Blackout', aims to DDoS the Root Internet servers | ZDNet

According to a note left by members of the Anonymous hacktivist movement on [Pastebin.com](https://pastebin.com), the group is planning to launch a distributed denial of service attack (DDoS) on the Internet's root DNS servers, using a Reflective DNS Amplification DDoS tool specifically created for 'Operation Global Blackout'.

More details:

We have compiled a Reflective DNS Amplification DDoS tool to be used for this attack. It is based on AntiSec's DHN, contains a few bug fix, a different dns list/target support and is a bit stripped down for speed.

The principle is simple; a flaw that uses forged UDP packets is to be used to trigger a rush of DNS queries all redirected and reflected to those 13 IPs. The flaw is as follow; since the UDP protocol allows it, we can change the source IP of the sender to our target, thus spoofing the source of the DNS query. The DNS server will then respond to that query by sending the answer to the spoofed IP. Since the answer is always bigger than the query, the DNS answers will then flood the target ip. It is called an amplified because we can use small packets to generate large traffic. It is called reflective because we will not send the queries to the root name servers, instead, we will use a list of known vulnerable DNS servers which will attack the root servers for us.

Since the attack will be using static IP addresses, it will not rely on name server resolution, thus enabling us to keep the attack up even while the Internet is down. The very fact that nobody will be able to make new requests to use the Internet will slow down those who will try to stop the attack. It may only lasts one hour, maybe more, maybe even a few days. No matter what, it will be global. It will be known.

Based on [a message update issued by Anonymous](#), the group has said that it still has the capability to target the Root Internet Servers.

Despite the fact that current Internet infrastructure allows the execution of [DNS amplification attacks](#), the Anonymous hacktivist movement is surely lacking the capabilities to execute such an attack, despite the high number of recruited users that may be participating in the attack.

For the time being, the [Low Orbit Ion Cannon \(LOIC\)](#) ICMP flooder, and the [RefRef web script](#) remain the primary attack tools used by the Anonymous hacktivist collective.

Learn more about [DNS Amplification attacks](#), what they are, how they work, and how can Internet Service Providers mitigate the threat posed by them.

'Anonymous' group attempts DDoS attack against Australian government | ZDNet

Following a threat posted on [YouTube](#) a month ago, the the well known malicious pattern of the "[Anonymous group](#) " failed to materialize earlier today when the group attempted to [launch a distributed denial of service \(DDoS\) attack](#) against the web sites of [Australia's Prime Minister](#) and the [Australian Communications and Media Authority's](#) web site as a protest against Internet censorship.

What tactics did they use, why it failed and who's behind it? Let's review the **09-09-2009.org** campaign , as well as **Operation Didgeridie** .

From a technical perspective, the attack was a [low-level crowdsourcing DDoS attack](#) that only managed to shut down the Primer Minister's web site for only a few minutes through multiple web requests run under several different threads, a standard feature for average denial of service tools.

Despite the campaigner's propaganda site descriptive enough to point out **09-09-2009.org** as the day for the attack, the use of link baiting for the purpose of increasing the load on a web server, usually has a short-lived effect, which is exactly what appears to have taken place earlier today.

Who's behind the attack, or may have something to do with the organizational efforts? Just like a previous case related to the "anonymous" group's DDoS activities on behalf of their members, where a [19-year-old teen pleaded guilty](#) for organizing the attack against the Church of Scientology, in this very latest attack, there appears to be a teen involved in the **09-09-2009.org** site.

The 09-09-2009.org Campaign

Data speaks for itself. A [cached copy](#) of the propaganda site from August, includes a link -- now removed -- to a MySpace profile ([myspace.com/andthesearethetemptation](#)) which is now redirecting to the profile of a 17-year-old teen from Australia who has

also posted a blog entry featuring "Anonymous" group's [propaganda video](#) .

A brief retrospective of the teen's attempt to monetize his MySpace popularity by offering to send MySpace bulletins -- spamming in this case -- to his users, indicates that he's been trying to do so since 2007, when he was offering to send [5 bulletins for \\$3 to 927 Friends!](#) under the same account, followed by another ad using the handle "AusieHerp" offering to send [150 friend requests for a dollar](#) .

It doesn't take a rocket scientist to establish a connection here, especially when the low-level crowdsourcing DDoS attack is theoretically in the arsenal of every 17-year-old MySpace rock star with 5773 (automatically added) friends on his profile, who's been monetizing their number since he was 15. Where the teen is clearly involved, the real coordination is happening from a publicly accessible Wiki under Operation Didgeridie.

[Next](#) -->

Operation Didgeridie

Operation Didgeridie consists of the distribution of DIY denial of service attack tools ([404ServerNotFound.exe](#)), launching "Fax bombs" using a [GetUp! Campaign script](#) , enticing into direct server compromise attempts by distributing a recently performed [web application vulnerability assessment](#) of Australian government web site using commercial tool.

The 'anonymous' group has been keeping a detailed log of the planning activities since August. Here's an excerpt from their planned/already executed points:

"It seems lots of people are confused as to what we are doing.

1) DDos the Prime Ministers website to get them the message about what is happening. 2) Get lots of Media Coverage to gain peoples attention and get everyone's support for taking the filter down. 3) Wait for their response: if it is yes, Stephen Conroy will resign, it's a win for us and the filter goes down. If they say no, we go IRL stuff here. Spread the word to everyone, hand out fliers. We

don't want this to be another peaceful hippie protest [Chanology] " OK, here's the plan that we seemed to settle on in the IRC.

1. On the 8th of August, 2009, the man with the video uploads it to Youtube and links it here youtube.com/watch?v=CEe7qhlFNs4). 2. We sort out scripts to 5-star, favourite it and such and send it straight to the top ASAP. 3. At the same time Anonymous notifies major news stations and such of the video. Essentially we want public and media attention on a huge scale. 4. Keep running your scripts intermittently during the month between 8/9/9 and 9/9/9. 5. The government responds to our message. 5.1. Spread their response to all the major Australian and worldwide media outlets. Quite a few of them should say something about it. 5.2. Upload a second one, addressed to the Australian public. Use metacafe and such as well. 6. The government DOESN'T respond in the month time frame. 6.1. We skullfuck their servers with the link in the UDP message. 6.2. We then wait again to see if they got the message. 6.3. If they respond, go to 5. 6.4. If they STILL don't respond, we call our /b/rethren in for a major DDoS on their central servers, and we flood Stephen Conroy's email address with viruses etc. 7. And so the war begins...

DDOS DOES NOT START AT 12 AM 9/9/09 AEST READ BELOW
People are being confused. This (DDOS) starts at 0900 GMT, EFG is all day, tell your friends, tell your family, tell your colleagues, tell your fucking cat. EXPLANATION : Extreme confusion between IRC, /net/ on 888chan and various other people has arisen over times. 0900 GMT is the time that the DDoS starts. The Government have until 9 am (2300 GMT) on the 9/9/09 to make their position clear. If they don't back down then Anon will attack. AKA 4 AM Eastern Standard Time."

Whereas the latest "anonymous" group DDoS attempt is a total failure, in its very nature crowdsourcing for launching DDoS attacks, of what's commonly referred as the "[people's information warfare concept](#) " proved to be a largely underestimated DDoS attack tactic during the last year.

From the [Russia vs Georgia cyber attack](#) (a combination of botnets and crowdsourcing), the [cyber attack launched by the Iranian opposition against pro-Ahmadinejad sites](#) (causing massive

disruptions without the use of botnets), next to the [Chinese hacktivists](#) that successfully [attacked CNN.com](#) in 2008 (crowdsourcing using **hackcnn.exe** DoS tool, iFrame refreshing sites), the [pro-Israeli crowdsourcing cyber attack](#) campaign (failed crowdsourcing attempt through **PatriotInstaller.exe**) [and the](#) 2007's "[Electronic Jihad Against Infidel Sites](#) " campaign (failed crowdsourcing due to badly coded app) - all of these campaigns clearly indicate that a well executed and coordinated crowdsourcing campaign makes the need for a botnet obsolete.

Android users hit by scareware scam | ZDNet

Security researchers from Kaspersky Labs have intercepted a [scareware variant targeting Android users](#), distributed as an Opera Virus Scanner.

According to Kaspersky:

Both web pages claim that the user's device might be infected and that somebody has access to personal data and then will ask the user to check his or her device for malware. If the user clicks on the button, the web page will emulate device scanning with the following 'hard-coded' results.

This web page never 'finds' malware on a SIM card but messages, calls, apps, browser history, storage and system files have threats, malware and are remotely accessible.

If the user clicks on the link, they'll be asked to download **VirusScanner.apk**, which is currently detected as Trojan-SMS.AndroidOS.Scavir. If the user is using a non-Android device, they'll be asked to download **VirusScanner.jar** currently detected as Trojan-SMS.J2ME.Agent.ij.

Malicious attackers are no strangers to the basics of localization and OS-porting. For instance, in the past we have seen [scareware templates localized to Arabic](#), and [DDoS bots ported](#) across multiple operating systems.

The migration of scareware also known as fake antivirus software to mobile platforms, was a logical development largely anticipated by industry watchers.

And the most popular password is... | ZDNet

It is "123456," based on the analysis of [32 million breached passwords](#) , obtained from [last month's RockYou.com server breach](#) , from which researchers from Imperva were able to analyze the insecure practices used by millions of users when choosing their passwords.

What did their analysis conclude? Short passwords, lack of lower-capital-numeric characters mix, and trivial dictionary words, which every decent brute forcing/password recovery application can find out in a matter of minutes.

Key findings include:

In just 110 attempts, a hacker will typically gain access to one new account on every second or a mere 17 minutes to break into 1000 accounts

About 30% of users chose passwords whose length is equal or below six characters

Moreover, almost 60% of users chose their passwords from a limited set of alpha-numeric characters

Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is "123456"

The rest of the passwords rated by popularity:

It's important to point out that, the same password "123456" also topped a similar chart based on [statistical analysis of 10,000 Hotmail passwords](#) published in October, 2009.

What actions on behalf of RockYou could have prevented this systematic practice of allowing end users to register with weak passwords?

Enforcing the use of stronger passwords as a long-term strategy, or borrowing short-term tricks from Twitter's, such as the "[banned passwords](#) " list consisting of 370 passwords that are not allowed to

be used during the registration process. And “123456” is at the top of the list.

Related: [Study: password resetting 'security questions' easily guessed](#)

For starters, the [32 million passwords were stored in an unencrypted format](#) , according to RockYou.com's announcement, and even if they weren't, the fact that the users were allowed to register with such weak passwords, makes it possible for someone to brute force them in a very short period of time once they gain access to the database.

Consider going through the [recommendations offered in the analysis](#) , but keep in mind that strong passwords as just as weak as weak passwords in general [if you're logging in from a malware-infected computer](#) .

Amnesty International UK compromised, serving exploits and malware | ZDNet

[Researchers from Barracuda Labs](#) have detected a drive-by malware campaign currently embedded at the web site of Amnesty International UK.

Based on historical data, the researchers conclude that the compromise took place on, or before Friday, December 16.

Once users visit the site, a malicious script will load from **3max[.]com** serving [CVE-2011-3544](#).

[Detection rate](#) for the malicious payload is low.

UPDATE: Emerson Povey from Amnesty International comments:

We have been working with our hosting service to resolve the problem. They have cleaned both servers, rebooted, and removed the script. At 2pm today they confirmed that the issue is now resolved.

Amazon's cloud services systematically exploited by cybercriminals | ZDNet

Security researchers from Kaspersky Labs have [spotted yet another SpyEye crimeware](#) variant using [Amazon's Simple Storage Service \(Amazon S3\) for command and control purposes](#).

According to a graph released by the vendor, cybercriminals are systematically abusing Amazon's service for command and control gateway, in an attempt to increase the average lifetime of the malware campaign.

This traffic camouflaging technique from a network perspective isn't new, what's new is the persistence shown in the graph in terms of systematically abusing the service.

Does [crimeware](#) in the [cloud](#) have a [future](#)? Most certainly, as cybercriminals appear to have been actively experimenting with the average lifetime for their malware campaigns, both, using rogue ISPs and netblocks, and legitimate cloud services, ultimately leading them to the conclusion that it's worth it.

AlertPay hit by a large scale DDoS attack | ZDNet

Timing is everything. Millions of account holders at privately owned [online payment gateway AlertPay.com](#) [weren't able to do business through the service](#) yesterday, due to the fact that AlertPay was under a large scale DDoS attack, according to a notice left by a company representative. Seven hours of downtime right in the middle of the [Christmas shopping season](#) with millions of businesses using the service affected, isn't coincidental. This DDoS attack, just like the [recent DDoS attack against a popular anti-fraud site](#), may have well been outsourced.

[AlertPay's statement on the situation](#) posted yesterday :

"We are currently experiencing a large scale DDOS attack that has hit our sites which started at approximately 6:00am EST Sunday. We are working with our data center to resolve and/or mitigate this issue. More information will be posted here as we get updates. For the time being customers can connect to AlertPay at an alternate location: <https://67.205.87.226>"

Several hours later, AlertPay issued [an update to the situation](#) :

"We have finally mitigated the massive DDOS attack that started at 6:00am EST. Unfortunately it took almost all day to resolve. The site is operational now, and hopefully we'll continue to tweak it more tomorrow to ensure this doesn't happen again. We sincerely apologize for the inconvenience and we understand that this outage affects each of you personally. We're sorry for that. We will continue to put measures in place so that outages like this do not occur again.

Ferhan"

There are two possible explanations regarding who's behind the DDoS attack. It's either unethical competition which in times of international economic meltdown can easily restore its market position by damaging the reputation and reliability of known competitor, or cybercriminals in "revenge mode" against a particular online payment processor that has detected their fraudulent activity,

thereby causing them huge monetary losses. Despite the fact that online payment gateways have always been targets for DDoS extortionists, with malicious attackers introducing new models like the DDoS for hire one, they have empowered literally everyone knowing how to contact them with the opportunity to forward the responsibility for an attack to a third-party. Here's a brief retrospective of DDoS attacks against online payment processors that took place during the last couple of years, with only a single instance of DDoS extortion :

[2004 - Worldpay's DDoS attack](#) [2004 - Authorize's DDoS attack](#)
[2004 - Authorize-It's DDoS attack](#) [2004 - 2Checkout's DDoS](#)
[extortion attack](#) [2006 - StormPay's DDoS attack](#) [2008 -](#)
[LibertyReserve's DDoS attack](#)

With DDoS extortion as a business model largely [replaced by](#)
[today's](#) DDoS for [hire services](#) , we're inevitably going to [witness](#)
[more attacks](#) throughout 2009.

Adobe's Serious Magic site SQL Injected by Asprox botnet | ZDNet

According to [SophosLabs](#) Adobe's owned [seriousmagic.com](#) has been [automatically SQL injected](#) by the Asprox botnet, becoming the very latest high profile legitimate web sites injected with links to exploits and malware serving sites :

"The infection, which resides at `hxxp://www.seriousmagic.com/help/tuts/tutorials.cfm?p=1`, instructs users browsers to silently install a malicious file from a series of domains known to host attack sites. Adobe [announced](#) its acquisition of Serious Magic two years ago and [whois records](#) indicate the company is the owner of the seriousmagic.com domain.

According to [this post](#) from anti-virus provider Sophos, Adobe was notified of the infected page on Friday. *The Register* visited the link (using a virtual machine, of course) on Thursday and found it was still trying to redirect users to a series of nefarious sites including `hxxp://abc.verynx.cn/ w.js` and `hxxp://1.verynx.cn/w.js`. While those links no longer appeared to be active, two other sites used in the attack, `hxxp://jjmaobuduo.3322.org/csrss/ w.js` and `hxxp://www2.s800qn.cn/csrss/ new.htm`, were still active at time of writing."

With [the asprox botnet](#) making an appearance at the sites of [Redmond magazine](#), and [Sony Playstation](#) in May and June respectively, **seriousmagic.com** is once again among the several hundred sites injected with the same malicious domains. Let's take a peek at this malware campaign, and see where it ends.

In short, every tutorial entry is SQL injected with a malicious domain, which means that if there are 60 tutorial entries, the malicious javascript loads 60 times ending up in an endless loop of redirections to other malware and advertising revenue earning domains set up in this campaign. More specifically, the malicious w.js attempts to execute a multitude of already patched client-side exploits, using the following structure and ultimately leading to a

copy of **Worm.Win32.AutoRun.qtg** with a high detection rate (29 AV scanners out of 36 detect it - 80.56%) :

www2.s800qn.cn /csrss/ new.htm www2.s800qn.cn /csrss/ flash.htm www2.s800qn.cn /csrss/ i1.htm www2.s800qn.cn /csrss/ f2.htm www2.s800qn.cn /csrss/ i1.html www2.s800qn.cn /csrss/ flash112.htm www2.s800qn.cn /csrss/ ff.htm www2.s800qn.cn /csrss/ xl.htm www2.s800qn.cn /csrss/ mi.htm www2.s800qn.cn /csrss/ real10.htm www2.s800qn.cn /csrss/ real11.htm bbexe.com /csrss/ rondll32.exe

Despite Adobe's delayed response and the fact that the domains are still active, they seem to have solved the issue by redirecting all traffic from the site to the clean adobe.com.

Adobe ships insecure version of Reader from official site | ZDNet

Following reports by users of Secunia's Personal Software Inspector on a potential false positive for an insecure version of Adobe Reader, [the company](#) has found that Adobe is surprisingly shipping the insecure Adobe Reader 9.1.0 version from [its official site](#) , potentially exposing users to previously fixed flaws in the latest 9.1.2 version.

Adobe's [comment on the issue](#) :

"Adobe says the the window of vulnerability is small because its updater tries to update Reader immediately and every seven days thereafter, automatically. However, the company acknowledges that the scenario suggested by Secunia -- clicking on a malicious PDF without Reader installed -- could lead to a compromised system."

Users are always advised to download software from its official web site in order to obtain the latest version of it, and avoid the potential security implications of downloading from an untrusted third-party web site. This case clearly demonstrates something else.

In particular, how in times when the [PDF file type remains among the most commonly used ones in targeted attacks](#) , next to the average [Internet user who isn't patching](#) wrongly [relying on antivirus software](#) for protection against the vulnerabilities posed by this practice, an insecure version of the software can in fact be downloaded from its official web site.

Asked to comment on the issue, PSI Partner Manager, Mikkel Winther says that: "PC users need to patch! They need to patch all their vulnerable programs and they need to do so as fast as possible after the patch has been issued from the vendor. Failing to do so is playing Russian Roulette with your IT security – it is only a question of time – and luck – when your system will be compromised."

Make sure that you're in fact running the latest [Adobe Reader 9.1.2](#) , and keep in mind that cybercriminals aren't exclusively using a particular vulnerability in an attempt to infect potential victims,

they're using everything there is at their disposal including historical vulnerabilities.

Adobe Reader 9 and Acrobat 9 zero day exploited in the wild | ZDNet

Yesterday, [Adobe confirmed the existence](#) of a critical vulnerability affecting [Adobe Reader and Acrobat](#) versions 9.0 and earlier, originally [detected by the Shadowserver Foundation last week](#) .

The ongoing targeted attacks have since been confirmed by both, [Symantec](#) and [McAfee](#) urging users to [disable JavaScript in Adobe Reader and Acrobat](#) until Adobe issues a patch on the 11th of March in the following way - **Click: Edit -> Preferences -> JavaScript and uncheck Enable Acrobat JavaScript** .

[Symantec's comments](#) on the potential for [massive attacks using the exploit](#) :

So far, these attacks appear to be targeted and not widespread. Symantec is continuing to monitor the vulnerability's use in the wild.

While examining the JavaScript code used for “heap-spraying” in these PDFs, we can see the same comments that show that these separate exploit attempts come from the same source! It seems likely that the people behind this threat are using targeted attacks against high-ranking people within different organizations—for example, locating the CEO's email address on the company website and sending a malicious PDF in the hope that their malicious payload will run. Once the machine is compromised, the attackers may gain access to sensitive corporate documents that could be costly for companies breached by this threat.

For the time being, cybercriminals chose to generate less noise by launching targeted attacks just like they did earlier this week using [IE7's MS09-002 vulnerability](#) . However, as we've previously seen it's only a matter of time until copycat attackers start using it on a large scale.

With several targeted campaigns currently active, what are the chances that a sample malware campaign would be once again monetizing infected hosts by infecting them with rogue security software similar to [Conficker's first release](#) ? Huge.

Go through related incidents using Adobe exploits: [MSN Norway serving Flash exploits through malvertising](#) ; [CNET's Client-side developer blog serving Adobe Flash exploits](#) ; [Rigged PDFs exploiting just-patched Adobe Reader flaw](#)

Upon analyzing the binary served once an infected host gets successfully exploited from a sample campaign, it's attempting to trick the user into installing the very latest rogue security software Spyware Protect 2009. The cute part is that the cybercriminals didn't manage to successfully configure their campaign resulting in a 404 error.

What's important to point out is that the original targeted attacks detected by the Shadowserver Foundation are once again using a well known and previously abused Chinese DNS provider (**js001.3322.org**) with more details about its owner available in a [related BusinessWeek article](#) .

Adobe posts workaround for clickjacking flaw, NoScript releases ClearClick | ZDNet

Following the recent release of a [PoC demonstrating clickjacking](#) in action, Adobe has [released a security advisory](#) offering [solutions for customers and IT administrators](#) on dealing with the flaw until they releases a Flash player patch before the end of October.

"We have just posted a Security Advisory for Flash Player in response to recently published reports of a 'Clickjacking' issue in multiple web browsers that could allow an attacker to lure a web browser user into unknowingly clicking on a link or dialog. This potential 'Clickjacking' browser issue affects Adobe Flash Player's microphone and camera access dialog. A Flash Player update to mitigate the issue will be available before the end of October. In the meantime, users can apply the workaround described in the Advisory."

And since [prevention is better than the cure](#) -- at least in the short term -- the just released [NoScript v1.8.2.1 aims to prove exactly the same with its ClearClick feature](#) :

"The most specific and ambitious is called **ClearClick** : whenever you click or otherwise interact, through your mouse or your keyboard, with an embedded element which is partially obstructed, transparent or otherwise disguised, NoScript prevents the interaction from completing *and reveals you the real thing* in "clear". At that point you can evaluate if the click target was actually the intended one, and decide if keeping it locked or unlock it for free interaction. This comes quite handy now that more dangerous usages of clickjacking are being disclosed, such as [enabling your microphone or your webcam behind your back to spy you through the interwebs](#) ."

Click in the clear, and [make sure you're not susceptible](#) to exploitation through [last quarter's security vulnerabilities](#) .

Adobe patches 6 critical security flaws in Shockwave | ZDNet

Today, Adobe released [Shockwave Player 11.6.8.638](#) that patches [6 critical security flaws in Shockwave](#) which could allow a malicious attacker the capability to inject malicious code into a system.

CVEs for the patched vulnerabilities - [CVE-2012-4172](#) , [CVE-2012-4173](#) , [CVE-2012-4174](#) , [CVE-2012-4175](#) , [CVE-2012-4176](#) , [CVE-2012-5273](#).

Next to updating to the latest Shockwave version, users are advised to ensure that they're not running outdated versions of their [third-party software](#) , [browser plugins](#) , to ensure that the URL they're about to visit is [a trusted one](#) , and take advantage of [application sandboxing techniques](#) to increase the probability for a successful prevention and contamination of a particular security threat.

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Active XSS flaw discovered on eBay | ZDNet

[According to XSSed](#), Indian security researcher Shubham Upadhyay has discovered an [active XSS flaw affecting Ebay.com](#).

The potential attacker would need an Ebay seller account, where he would [put XSS code into the HTML](#). The vulnerability could be used to trick users into trusting Ebay.com's reputable Web position in an attempt to serve client-side exploits to them. And that's just for starters.

Ebay.com is a [popular target](#) for malicious attackers, looking for ways to abuse and hijack the steady inflow of traffic hitting the site on a daily basis, and security researchers who on the other hand attempt to prevent abuse of the site by discovering and reporting security vulnerabilities to Ebay's Security Team.

[Mozilla Firefox's NoScript](#) proactively detects the XSS attempt, and blocks it.

The XSS flaw remains unfixed for the time being. eBay's Security Team has been notified.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Absolute Software downplays BIOS rootkit claims | ZDNet

Following a flood of calls from customers, the company behind [the LoJack anti-theft service](#) which researchers from Core Security Technologies recently portrait as a security threat, issued a statement [downplaying the researchers' claims](#) .

According to the statement, LoJack is neither a rootkit, nor does it behave in such a way. Moreover, the company insists that the product is forced upon any user, and that even if someone attempts to use it as an infection vector for a BIOS-persistent malware, traditional antivirus software will detect the attempt.

More from the [press release](#) :

Our BIOS module allows no special undetected path into the operating system. Uncontrolled access to a computer system may allow some BIOS images to be tampered with by an expert. Attempting to alter the Computrace BIOS module for malicious purposes will not defeat conventional detection as claimed by the authors. Any alteration to the BIOS module will cause any popular antivirus software to alert the customer.

More importantly, if the BIOS of a computer has been compromised by an attacker, that machine is exposed to innumerable other vulnerabilities far beyond the scope of the Computrace BIOS module. The presence of the Computrace module in the BIOS in no way weakens the security of the BIOS.

To a certain extend, every anti-theft service operates like malware since you wouldn't want the thief to be able to basically uninstall it while he's offline and then conveniently connect online without worrying that the victim will be able to trace them back. And even though the probability that current LoJack customers are already infected with malware that didn't took advantage of LoJack since it basically doesn't need to, is very high, [what the researchers really expose](#) is an anti-theft service which is trivial to deactivate and take

control of maliciously due to several points - [flawed update mechanism and lack of advanced self-protection mechanisms](#) .

Moreover, the company states that "*Computrace is designed to be activated, deactivated, controlled and managed by the customer using encrypted channels.* " Long gone are the days when a plain simple HTTP update mechanism using domain names, lack of digital signatures, combined with 8-bit XOR obfuscated configuration block can be described as encrypted channels. Going through the research presented by Alfredo Ortega and Anibal Sacco, the "encrypted channels" mentioned suddenly disappear:

Unpacked, the configuration block is easily modifiable. By simply changing the URL or IP, we can redirect the agent queries to our site. This is very easy to accomplish in the registry, but we don't have persistence for merely modifying the registry. To modify the configuration of the persistent agent we need to modify and reflash the BIOS. This is possible in many systems at the date of publication for this article, as unsigned BIOS are common.

For years, malware authors have been conducting network reconnaissance in an attempt to automatically prevent infected users from reaching the hard-coded update locations of antivirus software. [Conficker is the most recent example](#) of this fairly simple but highly effective approach.

Should LoJack customers worry? Common sense in the current threatscape will position the practice of hijacking the service for malware serving purposes as highly exotic one. But yes, the flaw is there. What the customers of the service should be really concerned with, is the ease with which a potential thief can block it from phoning back his location.

A U.S military botnet in the works | ZDNet

Make botnets, not war? In April, last year, [I asked the question](#) "Why establish an offensive cyber warfare doctrine when

you can simply install a type of Lycos Spam Fighting screensaver on every military and government computer and have it periodically update its hit lists?"

A year later, the U.S military is catching up on the concept, and with its current inability to utilize people's information warfare, is speculating on [a .mil hosts only botnet as an offensive cyber warfare capability](#). Sarcasm is also following, with suggestions for [Air Force 4-1-9 scams, and Dot mil phishing attacks](#). The controversial botnet idea leads us back to the [Make Love Not Spam campaign](#), which was perhaps the most successful people's information warfare campaign to date, DDoS-ing known spam sites.

Quote from [a related article](#) :

"America needs the ability to carpet bomb in cyberspace to create the deterrent we lack," Col. Williamson wrote. America faces increasingly sophisticated threats against its military and civilian cyberspace. At the same time, America has no credible deterrent, and our adversaries prove it every day by attacking everywhere. Some people would fear the possibility of botnet attacks on innocent parties. If the botnet is used in a strictly offensive manner, civilian computers may be attacked, but only if the enemy compels us. The U.S. will perform the same target preparation as for traditional targets and respect the law of armed conflict as Defense Department policy requires by analyzing necessity, proportionality and distinction among military, dual-use or civilian targets. But neither the law of armed conflict nor common sense would allow belligerents to hide behind the skirts of its civilians. If the enemy is using civilian computers in his country so as to cause us harm, then we may attack them."

Protecting the "everywhere" is very marketable if you're a defense contractor pitching products and services to new hires, but reality is

different, "everywhere" is a utopia by itself. Moreover, prioritizing the DDoS attack that would follow based on dual-use, civilian or military targets renders the entire idea pointless, since a DDoS attack could be launched from a foreign country's major university network, falling into the dual-use systems category. From a historical perspective, international adversaries are also known to enjoy hiding behind "the skirts of the civilians", by building barracks next to schools, headquarters next to hospitals, or building a ghost infrastructure within the urban landscape, right under the nose of civilians themselves, used as bites and insurance for causing complexity in any upcoming attacks.

Some issues to consider:

cyber warfare tensions engineering in the sense of making it look like a specific country is attacking the U.S military in order to have the U.S military DDoS the country on behalf of the malicious parties, a fully realistic scenario given the huge number of malware infected hosts and the bad guys Geolocation capabilities

with the number of [netblocks prone to IP spoofing](#) , there's no accountability on who's attacking who if someone wants to achieve the effect, well try everyone

from another perspective the idea is both, ingenious and easy to render pointless if it is to include only .mil hosts within the botnet, mostly because a .mil tld extensions are descriptive enough to be blocked by default, and so are all the publicly known military netblocks

knowing that the U.S military would DDoS back anyone attacking its networks creates opportunities for forwarding the execution of DDoS attacks to someone who's thinking they're under attack as [botnets for hire](#) consisting of [infected hosts from a specific country only](#). are already pitched by botnet masters themselves

Here's one favorable comment of a reader :

"Whether or not we actually need a "botnet" to do it is inconsequential. DDoS attacks can be very useful when used in a coordinated IW attack on enemy communications and network infrastructure."

Where's the enemy, and where's the enemy's communications and network

infrastructure at the first place? It's both nowhere, and everywhere, and you cannot DDoS "everywhere", and even if you waste a decade building up the capability to DDoS everywhere, your adaptive enemy will undermine the resources, time and money you've put into the process by avoiding outside-to-inside attacks, and DDoS your infrastructure from inside-to-inside. Will you, now that you have the capability, DDoS your homeland's infrastructure given that it is the original source of the attack against the homeland in general? Having the capability to do something, does not mean that capability is applicable at all. The stereotype of conventional military thinking that both armies will just round up, set up C&C headquarters is precisely what [unrestricted warfare](#) is undermining. [Autonomous people's information warfare](#) , [self-mobilizing hacktivists](#) , distributed management without a central coordination point, doesn't leave a lot of targets to bomb or DDoS.

The bottom line - why put efforts into building something that would generate a lot of negative publicity and might never materialize, when you can basically outsource the process and have the capability provided on demand? Just like the bad guys who do not have access to botnets do by using botnets as a service?

A security company wants you to DDoS its servers | ZDNet

"There is no such thing as bad publicity except your own obituary "
- Brendan Behan. [Ypigsfly](#) , a company describing itself

as a group of seasoned veterans of the Internet network infrastructure business, has just launched [Killthisbox.com](#) , a DDoS challenge enticing you to knock down the site for 15 minutes in exchange for a fifty dollar gift certificate from the well known geeky outlet ThinkGeek.

Are the folks behind this challenge really trying to test their new DDoS protection system, or is this a case of a guerrilla marketing approach aiming to promote the DDoS mitigation services of the company by creating controversy?

Considering the non-technical description of the contest, as well as the lack of a detailed explanation of what constitutes "knocking them off the Internet", I think it's a marketing campaign that would inevitably attract negative publicity. Perhaps with a reason, taking into consideration the fact that the challenge [stimulates others to build DDoS capacity](#) or learn how to by providing a rather modest reward.

Moreover, none of the eventual participants would be able to imitate a realistic DDoS attack on **target.killthisbox.com** and knock it offline, unless of course they are real botnet masters who I doubt would waste their botnet's bandwidth in order to participate in the challenge. And even if the company's objective is to gather realistic data on the DDoS threatscape, having end users trying to DDoS you wouldn't provide the company with a realistic picture, and will also put the end users into the position of attackers abusing their network's resources - if detected and approached by their ISP. These are the rules of the DDoS challenge :

"1. Register a day and time of your attack along with your Handle and unique password 2. Try and knock this site off the Internet for 15 minutes, anyway you can 3. If you can, email us with your handle

and unique password, name and address and we will send you your prize 4. No we are not trying to find out who you are and send the Authorities to your house, we are just testing a DDOS defense system"

Going through [the real-time attack stats](#) , you'll see end users doing nothing else but getting themselves in trouble, at least so far. I wonder is their upstream provider Peer 1 Network Inc even aware of the competition, and what's their Network Operations Center take on it?

A patched browser - false feeling of security or a security utopia that actually exists? | ZDNet

Kaspersky Lab's recently released "[Global Web Browser Usage and Security Trends](#)" report sparks several important questions from a security perspective:

Does the fact that (according to the study and [third-party metrics services](#)) Google's Chrome has the largest market share, make the Internet any safer?

Does it really matter if Chrome users get the latest updates delivered to them, in an attempt by Google Inc. to shorten the "window of opportunity" for a malicious attacker to take advantage of the security vulnerabilities that could be exploited in the old version of the browser?

[Is Chrome the most secure browser on the market?](#) What's the current situational reality in respect to the most commonly used tactics by cybercriminals attempting to infect a targeted host, and is a version of a particular browser relevant to their practices?

Let's start from the basics.

Years ago, cybercriminals took advantage of the fact that, due to usability issues, [browsers were basically shipped insecure by default](#) in an attempt not to ruin the Web experience of the user. Back in the day, [cybercriminals still relying](#) on inefficient [isolated exploitation attempts](#), could not achieve the "[malicious economies of scale](#)" evident across the entire cybercrime ecosystem in 2012, as far as client-side exploitation is concerned.

It all changed with the releases of the [RootLauncher Kit](#), the [WebAttacker Kit](#), [MPack](#) and [IcePack](#), which revolutionized the [systematic client-side exploitation of end points](#), shifting the attention of cybercriminals to the average Internet user still living in a "free adult content leads to viruses" world.

Although the shift towards client-side exploitation has been evident ever since the [continues release of numerous Web malware exploitation kits](#) throughout 2012, social engineering tactics continued to proliferate, potentially undermining the built-in security mechanism implemented in any browser. A socially engineered user will manually bypass any "security warning screen", or may even click further to get what he clicked for originally, even though he received a clear warning for the maliciousness of a site in question, through, for instance, Google's SafeBrowsing initiative. Which on the other hand [mitigates a certain percentage of the risk](#) of getting exploited through client-side vulnerabilities, but as we've already seen in the latest version of the Black Hole Exploit Kit 2.0, cybercriminals are adapting to the process by [cloaking the malicious content](#), and not displaying it to Google's crawlers.

Just how prevalent are social engineering driven attacks nowadays? According to Microsoft's Security Intelligence Report for 2011, [the most popular malware propagation tactic is the one that requires user interaction](#). Although the report is emphasizing on the rather insignificant activity in client-side exploitation, it excludes the fact that over the past couple of years cybercriminals have been combining social engineering and client-side exploitation in an attempt to increase their visitor-to-malware-infected-victim rates.

Yet another important aspect of a browser's security that has the capability to bypass the built-in security mechanisms, are browser extensions. On [numerous](#) occasions [we've seen](#) successful campaigns relying on [bogus browser extensions](#) for Firefox and [Chrome](#), which don't even attempt to exploit a particular browser specific vulnerability besides socially engineering the user. Although [Google reacted to this trend](#) in July 2012, social engineering attacks still remain possible.

What are cybercriminals emphasizing on in 2012? Massive client-side exploitation, or social engineering driven malicious campaigns? Not surprisingly, on both. However, despite OS/Software specific Patch Tuesdays, [cybercriminals don't tend to exploit zero day flaws](#), instead, they exploit outdated vulnerabilities in third-party

applications and browser plugins, leaving a lot of users with fully patched browsers with a false feeling of security.

Are average Internet and corporate users actually patching their third-party applications and browser plugins in general? Not even close.

According to publicly obtainable data, [patched vulnerabilities remain the primary exploitation vector](#) for cybercriminals to take advantage of. During the time the data was gathered (2011), [37 percent of users browsing the Web with insecure Java versions](#) and [56 percent of enterprise users using vulnerable Adobe Reader plugins](#), the majority of which were [exploiting vulnerabilities in Adobe's products, followed by Sun's products](#).

Running Chrome due to its built-in [secure by default sandboxing technologies](#), running Firefox due its compatibility with [NoScript](#), running [Internet Explorer](#) due to its [acclaimed](#) invincibility to [social engineering attacks](#), or running Opera or Safari due to their small market share making it -- theoretically and practically -- a less valuable target for cybercriminals to attack, only mitigates a certain percentage of the risk of getting infected with malware, and are only part of the [Defense-in-Depth concept](#).

What do you think? Does a fully patched browser offer total security, or does it basically mitigate only a certain percentage of the risk? Which browser are you currently running? Is it the latest version? Do you feel secure with it, or is it giving you false feeling of security, and you know it? When was the last time you checked whether you're running the latest version of your [browser plugins](#), and [third-party software](#), or are you still obsessed with Patch Tuesdays as the corner stone of ensuring your security online?

TalkBack!

Find out more about Dancho Danchev at his [LinkedIn profile](#).

9/11 related keywords hijacked to serve scareware | ZDNet

Anticipating the [logical peak](#) of 9/11 [related keywords](#) on the [8th anniversary](#) of the attacks, cybercriminals have hijacked the trending topic by occupying thousands of related keywords for the purpose of [serving fake security software](#) .

None of the sites are currently marked as harmful by the SafeBrowsing initiative, due to the evasive tactics applied in the campaign, with the majority of them already appearing within the first twenty results.

Is this a deliberate 9/11 themed blackhat SEO campaign, or is it "*blackhat SEO for scareware serving purposes as usual* " type of campaign?

The very same Ukrainian cybercrime group -- [detailed assessments](#) of their [ongoing campaigns](#) confirm their [use of Google Trends](#) -- that was recently [hijacking Obama Speech related keywords](#) next to [U.S Federal Forms keywords](#) , is also the same group behind the current 9/11 themed campaign.

Whereas it would first appear that they are very good at picking up trending, and very recent topics manually, the reality is that the [process is completely automated](#) , and has been for the past couple of years. This dynamic traffic hijacking in a near real-time Web is already undermining the usefulness of static lists of "[dangerous keywords](#) " or "[dangerous celebrities](#) " to search for.

Go through related posts: [Cybercriminals hijack Twitter trending topics to serve malware](#) ; [Cybercriminals syndicating Google Trends keywords to serve malware](#) ; [Google Video search results poisoned to serve malware](#) ; [Massive comment spam attack on Digg.com leads to malware](#)

Compared to previous blackhat SEO campaigns, the campaigns launched by this group over the past couple of months indicate a lot of planning activities taking place before launching it. For instance, the malware, the redirection domains and the scareware domains

are rotated once or twice every 24 hours in an attempt to increase the campaign's lifecycle.

The latest campaign is pushing [Scanner-137082_2007.exe](#) , and while its generic detection rate will inevitably improve, not falling victim to a scam that's selling non-existent security software, remains the best move.

90,000+ pages compromised in mass iFrame injection attack | ZDNet

Security researchers from Armorize have intercepted a currently [live mass iFrame injection attack](#), affecting over 90,000 Web pages.

Once the users visits an affected page, a number of javascript redirectors lead the user to a client-side exploits serving page.

How did the attack take place? Malicious attackers are either [abusing input validation flaws](#) within the vulnerable sites, or have been [harvesting botnets](#) for [stolen FTP credentials](#) in order to embed the pages with the malicious iFrame.

Go through related posts:

[More High Profile Sites IFRAME Injected ZDNet Asia and TorrentReactor IFRAME-ed Massive IFRAME SEO Poisoning Attack Continuing More CNET Sites Under IFRAME Attack Wired.com and History.com Getting RBN-ed Embedding Malicious IFRAMEs Through Stolen FTP Accounts Embedding Malicious IFRAMEs Through Stolen FTP Accounts - Part Two Injecting IFRAMEs by Abusing Input Validation](#)

The iFrame domain *willysy(dot)com* is currently flagged as malicious.

75% of online banking sites found vulnerable to security design flaws | ZDNet

In a paper entitled "[Analyzing Web sites for user-visible security design flaws](#)" to be published at the Symposium on

Usable Privacy and Security meeting at Carnegie Mellon University July 25, Atul Prakash and two of his doctoral students [examined 214 financial institutions in 2006](#), finding that over 75% of all the sites have at least one security design flaw :

"These design flaws aren't bugs that can be fixed with a patch. They stem from the flow and the layout of these Web sites, according to the study. The flaws include placing log-in boxes and contact information on insecure web pages as well as failing to keep users on the site they initially visited. Prakash said some banks may have taken steps to resolve these problems since this data was gathered, but overall he still sees much need for improvement.

"To our surprise, design flaws that could compromise security were widespread and included some of the largest banks in the country," Prakash said. "Our focus was on users who try to be careful, but unfortunately some bank sites make it hard for customers to make the right security decisions when doing online banking."

What are the security design flaws they found, and how easy are they to exploit on a large scale compared to web application vulnerabilities within the banking sites, or even indirect attacks against the banks by attacking the weakest link in the process, the malware infected customer in this case?

They seem to have found what they were looking for in general, flaws like the following :

- Placing secure login boxes on insecure pages
- Putting contact information and security advice on insecure pages
- Having a breach in the chain of trust: When the bank redirects customers to a site outside the bank's domain for certain transactions without warning
- Allowing inadequate user IDs and passwords: Researchers looked

for sites that use social security numbers or e-mail addresses as user ids

E-mailing security-sensitive information insecurely

Perhaps two of the key findings are the lack of SSL sessions at thought to be "secure login boxes" found at 47% of banks, and even more disturbing the fact that certain banks would use a customer's social security number as a user ID. It would be interesting to see who's who in all of these insecure practices once the research gets published online later this week.

In every day's reality through, when cyber criminals aren't capable of exploiting [web application vulnerabilities within the Ebanking sites](#) that would assist them in their phishing attempts, what they would do in order to cause the speculated losses of billions of dollars, is attack the customer whose once [malware infected computer is no longer to be trusted](#) for any type of transactions, [no matter of the type of security measure used](#) .

56th variant of the Koobface worm detected | ZDNet

Researchers from [PandaLabs](#) are reporting on the detection of the 56th variant of [the Koobface worm](#) (Boface.BJ.worm), spreading across Facebook, Tagged, Friendster, MySpace, MyYearBook, Fubar.com, Hi5 and Bebo since May, 2008.

According to the company, the growth of [Koobface related infections](#) is as high as 1,200% since the first time it was detected over an year ago, where almost 40% of the infections based in the U.S, with [the growth trend](#) also confirmed by [Microsoft's Malware Protection Center](#) .

What the cybercriminals have changed this time is the template, the use of an Ukrainian web site hosting service, and the "missing" fake codec, which upon execution is not only converting the infected PC into a hosting provider part of the campaign, but is also pushing scareware, **liveantimalwareproscanner .com** and **live-antimalware-scanner .com** in particular.

Despite the [ongoing industry collaboration](#) , and with [MySpace already declaring victory over Koobface](#) , the persistence of the malware gang using social engineering tactics, [typosquatting of social networking domains](#) , and their [outsourcing of the CAPTCHA breaking process](#) aimed to [slow down automated abuse](#) of the sites, makes Koobface a success story (see sample [statistics](#)) that you should keep an eye on.

56 percent of enterprise users using vulnerable Adobe Reader plugins | ZDNet

According to Zscaler's most recent "State of the Web" security research report, 56.46% of enterprise users running Adobe Reader have outdated version installed, making them susceptible to client-side exploitation kits courtesy of web malware exploitation kits such as the [Blackhole Exploit Kit](#) which targets vulnerabilities in Adobe Reader and Java.

"Patching and updating is key to security as many attacks now target outdated plug-ins. In fact, recent large hacks making headlines are thought to have been performed by compromising just one plug-in in an enterprise," said Michael Sutton, VP security research at Zscaler .

Not surprisingly, cybercriminals are quick to adapt. Thanks to the modular nature of web malware exploitation kits, they can add exploits targeting a particular exploitation vector at any time. In this case, Adobe Reader will be exploited "in between" the rest of the client-side exploits available at the disposal of the malicious attacker.

The research findings were also confirmed in a separate study conducted by Avast. In it, the researchers found out that [6 out of every 10 users run vulnerable Adobe Reader](#).

So, what are you waiting for? [Check whether you're running vulnerable plugins](#) susceptible to client-side exploitation, and patch them right away.

500,000 stolen email passwords discovered in Waledac's cache | ZDNet

Closely monitoring the [post-take down](#) activities of the Waledac botnet, security researchers took a peek inside the botnet's cache of stolen accounting data, and found half a million stolen email passwords, next to hundreds of thousands of stolen FTP passwords.

[More info:](#)

"More specifically, they have 123,920 login credentials to FTP servers at their disposal. This number is significant, considering the Waledac controllers use an automated program to login to these servers and patch (or upload) specific files to redirect users to sites that serve malware or promote cheap pharmaceuticals.

We also discovered 489,528 credentials for POP3 email accounts. These credentials are known to be used for "high-quality" spam campaigns."

Abuse scenarios

Stolen email accounts can be used for email impersonation attacks abusing the trust chain between the owner and a countless number of services and contacts related to him. Once [the trust chain has been abused](#), the malicious attackers can also easily [embed the accounting data](#) into their [spam platforms](#), in an attempt to take advantage of the [DomainKeys ecosystem](#) and increase the probability of reaching the user's Inbox.

The stolen FTP accounts are usually embedded in [efficiency-driven blackhat SEO](#) (black hat search engine optimization) tools, and managed spam/exploits-serving services, allowing the malicious attackers to easily tailor their campaigns, be it pharmaceutical scams, pure blackhat SEO campaigns with real-time syndication of trending topics across the Web, and, of course, serving client-side exploits through legitimate web sites.

See also:

The current state of the crimeware threat - Q&A Embedding Malicious IFRAMES Through Stolen FTP Accounts Embedding Malicious IFRAMES Through Stolen FTP Accounts - Part Two

This is perhaps the perfect moment to change your passwords -- in a perfect world best practices are in place -- from a malware-free host.

5 reasons why the proposed ID scheme for Internet users is a bad idea | ZDNet

Imagine waking up in a world, where you would need to use [two-factor authentication/biometric based ID](#), in order to do anything online. The reason for this? Accountability and supposedly, prevention of cybercrime.

This may well sound like the long-term reality, but Kaspersky's [CEO Eugene Kaspersky](#) has been pushing the idea for years. [According to a recently published article](#), he still believes that the time has come for a mass adoption of hardware IDs affecting every Internet user.

Here are five reasons why I think this is a bad idea, if not one that is virtually impossible to implement.

"To prevent the misuse of social networking accounts, Kaspersky is pushing the idea of government IDs as a prerequisite for all computer users. "I've been talking about this for four years already, that we need to have a secure design for the (entire) internet," he says. In Kaspersky's perfect world, all digital citizens would carry some form of ID to go online, hopefully creating greater hurdles for malware creators - but creating a nightmare for privacy advocates."

"When you buy a car, the car is registered and you have a drivers licence. If you want to have a gun, the same thing - it's registered to the person who bought it. The question is why? Because it's dangerous. With computers, you can make much more harm than with a gun or car."

At first, the proposed ID scheme seems pretty logic in terms of accountability. Here are five points on what's wrong with it.

Privacy vs Security for the sake of accountability - Interestingly, Kaspersky isn't claiming that the ID scheme would somehow lead to more privacy being sacrificed on behalf of the users. Instead, he argues that privacy is already dead, and that your ISP already knows everything about you, therefore the use of hardware IDs shouldn't really have an [impact on the end user](#),

[since he's losing nothing](#). If privacy is already dead, and an ISP somewhere across the globe always knows everything about the activities of its customers, then what's [the point of having a hardware based ID](#) to authenticate something that's (supposedly) already known? There isn't. Which leads us to the best possible solution to the problem of tracking down the source of a cybercriminal - cross-border/cross-agency threat intelligence sharing.

Mass adoption of two-factor authentication is no proof that it works, exactly the opposite - Using the "success" of two-factor authentication for E-banking as an example on the usefulness of the proposed IDs is partially incorrect. How did cybercriminals manage to undermine the myth of the hardware based authentication? Not by attempting to attack it directly, but by bypassing it entirely in the sense of patiently and automatically waiting for the now authenticated victim to start interacting with the E-banking provider. Neither a SSL connection, nor a [two-factor authentication device would prevent a crimeware-infected host from](#) having its owner victimized by cybercriminal on the other side of the world. In the worst case, it would offer the user a false feeling of security.

Hardware IDs would not solve the problem, since a malware infected host will be used to commit the same crimes - The article claims that the ID scheme would create some sort of hurdle for malware authors, which is totally untrue. How come? Even if we assume that the end user would be unplugging himself/herself from the Internet and connectivity would be disabled unless he authenticates himself again, botnet masters would continue operating with the bots whose users are online, taking advantage of the different time zones. With or without the hardware ID, the malware-infected host would continue forwarding the responsibility for the actions of the actual cybercriminal, to the owner of the host, unless it's proven the same has been compromised. Long gone are the days when a cybercriminal would use his own host to commit the crimes, unless we exclude [the Mariposa botnet masters of course, who got caught by doing exactly the same](#).

By authenticating yourself on a PC that's not yours, you automatically inherit its reputation - A [quote from the article](#) -

"Kaspersky says that in Dubai "they are going to introduce regulations that in public places, to get access to public WiFi, you have to present your ID. " The idea is that whenever a phishing attack is launched from a particular host, using the proposed ID scheme would allow law enforcement to find out the person that's supposedly behind the campaign based on the fact that he's already authenticated himself. In reality though, even when you're using a public computer, the malicious campaigns that were going on in the background would continue taking place, with numerous users identifying themselves, and none of them would theoretically have anything to do with these background processes maintained by someone on the other side of the world.

Budgeting the idea on an international scale is off base - In order for this ID scheme to get even close to being of any use, would be its mass adoption. Otherwise, certain countries that deny, do not have the resources, or don't even believe in the idea, wouldn't bother implementing this. The real problem with fighting cybercrime has never been about the lack of technologies or knowledge on how the ecosystem really works. It's always been about the lack of mass adoption for these technologies, and the lack of active cooperation among countries. Even if we assume that in a perfect world, this scheme gets implemented, just like [photoshop-ed IDs sent to domain registrars](#) in Russia and China in order to comply with new regulations, [biometric passports have been under fire](#) since day one. It would be totally naive to assume that the same wouldn't happen to these IDs as well.

Do you think the pros of the proposed hardware based ID scheme -- if any -- are worth the loss of privacy? Do you still believe privacy exists online? Are you willing to sacrifice even the left overs of it, with the idea to improve accountability over the Internet, and supposedly limit cybercrime?

How long before cybercriminals undermine the ID scheme as well, and wouldn't a potential flaw in it lead us the same situation we're into today - millions of end users still susceptible to outdated 3rd party application flaws and vulnerable browser plugins, given the fact that only a small number of the hardware ID users would even know they're susceptible to impersonation based on the flaw?

Talkback.

Cartoon courtesy of Clay Bennett.

44% of second hand mobile devices still contain sensitive data | ZDNet

According to [a recent research conducted by BT, the Edith Cowan University, and the University of Glamorgan \(Wales\)](#) , 44% of the 160 second-hand devices that they tested, still contained sensitive data such as bank accounts, board meetings, business plans, and financial data. Using the data obtained, their analysis indicated a greater risk of espionage for the organizations the owner works for, than for the individuals themselves, once again proving that users don't erase the data on their devices before selling them, thereby acting as the weakest link.

The potential for abuse in the form of corporate espionage, unethical competitive intelligence, business sabotage and blackmailing will naturally increase, following the high number of lost mobile devices with ever increasing capacity and the lack of basic security awareness on the user's end.

"New research finds 44 per cent of second-hand devices still contain sensitive data Over a third of BlackBerry devices are sold without being wiped of sensitive personal and corporate data, according to new research released today by BT. The study of over 160 second-hand handheld devices found they still contained details of bank accounts, board meetings and financial data. Nearly a quarter of phones contained information which could allow the previous owner and employer to be identified, while 43 per cent of BlackBerrys contained information which could pose a significant risk to organisations if exposed."

What type of data were the researchers able to access? Starting from [salary details, financial company data](#) , bank account details, sensitive business plans, and personal medical details, and going to [bids and contracts under negotiations](#) , uncomplimentary comments about employees, an extensive list of contacts and a complete log of phone calls and diary commitments, in between evidence of an ongoing affair between a man and a woman :

"According to Godfrey at Sims Lifecycle Services, a discarded, unwiped phone or PDA is "a perfect tool for social engineering, and it's only going to get worse" as the storage capacity of mobile devices increases. He says: "The point of this work is really to bring that across to people the risks that mobile phones present to their personal data." Of the devices in the survey, 7% had enough personal data on them for the individual concerned to have their identity stolen, and 7% would have allowed a corporate fraud to have taken place. Another 2% still had Sim cards in them, while 27% of the BlackBerrys in the survey had company data and 16% carried personal information."

In case you wouldn't feel that very comfortable being in the center of a corporate espionage scandal, or have your private life exposed to someone that could figure out a way to monetize your private life by blackmailing you - wipe your private data before selling your device.

419 scammers using NYTimes.com 'email this feature' | ZDNet

What do Burkina Faso and the [New York Times](#) have in common? As of recently, a peak of 419 scams promising you the Moon and asking you for [advance-fees](#) via emails sent through the NYTimes.com's 'email this feature' in order to successfully bypass anti-spam filters.

The tactic applied by 419 con artists aiming to abuse the clean IP reputation of NYTimes.com's email servers has been persistently diversifying the themes and user names of registered users [during](#) the [last](#) couple of [months](#) . Interestingly, upon interacting with the scammers, all campaigns seem to be operated by the [same gang](#) using the [ONATEL ISP](#) based in Burkina Faso.

Here's how the scheme works:

Their business model is in fact a primitive version of the [scareware business model](#) relying on [affiliates to drive traffic](#) and infect people.

In this particular campaign, Alizeta Ouedraogo acts as an affiliate which is spamming and interacting with the potential victims, where once they fall into her scenario she'd basically redirect them to a third-party and insist that you use "*DONATION FROM MRS.ALIZETA OUEDRAOGO* " as a subject of your email so that she/he can later on have a claim on the money obtained :

"If you agree with me in respecting my last wishes as listed in this message, then you go ahead and contact my attorney through his email and phone: His name is Hon.Sanfo A.Karim, his Email: sanfoabdulkarim@yahoo.fr phone: +22676578847. While contacting him use, (DONATION FROM MRS.ALIZETA OUEDRAOGO) as your subject, this will enable him to know your purpose of communicating. I am looking forward to hearing from you again."

Needless to say that this is a scam you should not interact with.

419 scammers using Dilbert.com | ZDNet

Scammers too, know [Dilbert](#) .

On their way to search for clean IPs through which to send out yet another scam email, 419 con-artists (Mrs Sharon Goetz Massey) have recently started using Dilbert.com's recommendation feature in an attempt to bypass anti-spam filters -- and it works. The use of Dilbert.com's clean IP reputation comes a month after [419 scammers used the same tactic on NYTimes.com 'email this' feature](#)

Isolated incidents or an indication of a trend? 419 scammers are like spammers circa 1997, technically unsophisticated but fully capable of [maintaining a fraudulent infrastructure by using legitimate services only](#) .

Case in point - [automatically registered email accounts next to compromised ones](#) already represent the source of a close to [20% of the overall spam volume](#) , and these levels remain steady. A logical question arises, why hasn't 419 advance-fee fraud reached the efficiency levels of phishing or spam in general, taking into consideration the fact that [spam is already outsourced as a process](#) ? It's because South Africa-based scammers lack the networking skills necessary to approach international cybercrime groups which would not only manage the entire scamming process for them, but would help them improve the quality of the campaigns.

Data detailing the magnitude of advance-fee fraud varies. According to the [U.S Internet Crime Complaint Center](#) , Nigerian letter fraud represented a 5.2% of the total loss reported in their annual 2008 report, with non-delivery scams topping the chart. Internationally, the number of [advance-fee fraud cases](#) and the number of victims is higher:

In the last two years, the [Electronic and Financial Crimes Commission \(EFCC\)](#) of Nigeria has been putting scammers in jail. The commission has invited journalists on a successful high-profile operation to apprehend a scamming ring and has helped foil

Nigerian-led groups that ran multimillion-dollar fraud schemes. In a 2007 report, the EFCC said it handled more than 18,000 advanced-fee fraud cases, a six-fold increase in just four years.

From a technical perspective, advanced-fee fraud is still in its infancy, however the results of its tactics are pretty evident in the face of the thousands of scammed people across the globe. Don't be one of them, [spot the scam](#) , take a minute and [report it](#) .

37 percent of users browsing the Web with insecure Java versions | ZDNet

Over a period of three months, researchers from CSIS have monitored 50 different exploit kits on 44 unique servers, and found out that [31.3 % were infected with the virus/malware](#) due to missing security updates.

In particular, users were running outdated versions of specific applications and browser plugins. Java JRE accounted for 37 percent of the most vulnerable applications, followed by Adobe Reader/Acrobat with 32 percent and Adobe Flash with 16 percent.

Common vulnerabilities exploited by cybercriminals in their [web malware exploitation kits](#) include:

CVE-2010-1885 Microsoft Help & Support HCP CVE-2010-1423 Java Deployment Toolkit insufficient argument validation CVE-2010-0886 Java Unspecified vulnerability in the Java Deployment Toolkit component in Oracle Java SE CVE-2010-0842 Java JRE MixerSequencer Invalid Array Index Remote Code Execution Vulnerability CVE-2010-0840 Java trusted Methods Chaining Remote Code Execution Vulnerability CVE-2009-1671 Java buffer overflows in the Deployment Toolkit ActiveX control in deploytk.dll CVE-2009-0927 Adobe Reader Collab GetIcon CVE-2008-2992 Adobe Reader util.printf CVE-2008-0655 Adobe Reader CollectEmailInfo CVE-2006-0003 IE MDAC CVE-2006-4704 Microsoft Visual Studio 2005 WMI Object Broker Remote Code Execution Vulnerability CVE-2004-0549 ShowModalDialog method and modifying the location to execute code

Go through related posts:

[56 percent of enterprise users using vulnerable Adobe Reader plugins](#) [Kaspersky: 12 different vulnerabilities detected on every PC](#)

Verify your Java version [here](#), ensure that all of [your plugins](#) and [software applications](#) are up to date in order to mitigate the risks posed by the existence of web malware exploitation kits.

300 Lithuanian sites hacked by Russian hackers | ZDNet

A recently accepted [legislation in Lithuania banning communist symbols](#) across Lithuania, has prompted Pro-Russian

hackers to start defacing Lithuanian sites, an indication of the upcoming attack was detected last week with [active discussions around Russian forums](#) greatly reminding us of the Russia vs Estonia cyberattack sparked due to the removal of a Red Army memorial from the capital Tallinn. [More info](#) :

"Unidentified hackers broke into several hundred Lithuanian Web sites over the weekend, plastering them with communist symbols, government officials said Monday. The hackers posted Soviet symbols -- the hammer and sickle, as well as the five-pointed star -- and scathing messages with profanities on Web sites based in the ex-Soviet nation, officials said.

"More than 300 private and official sites were attacked from so-called proxy servers located in territories east of Lithuania," said Sigita Jurkevicius, a computer specialist at Lithuania's communications authority. The hackers hit Web sites from both the government and private sector, including the Baltic state's securities commission and ruling Social Democratic Party. Others included a car dealership and a grocery chain."

Was this a warning sign for an upcoming DDoS attack, and would other Baltic countries also start getting attacked according to their ongoing discussion online?

Let's start from where the campaign started - across web forums. A week ago, the Estonian television ETV24 reported that they've started coming across multiple appeals from novice hackers to launch a large scale DDoS attack against Latvian, Ukrainian, Lithuanian and Estonian sites. According to Lithuanian researchers, [the hackers used compromised hosts](#) in France and Sweden in order to execute the defacements, and even more interesting is the fact that pretty much all of 300 defaced web sites were hosted on the

same ISP, [Hostex, previously known as Microlink](#) , indicating that a mass web site defecement took place.

In times when [launching a DDoS attack](#) doesn't require having access to botnet, since [the attack can be outsourced](#) and requested as a service, someone can literally engineer cyber warfare tensions by abusing the momentum and making it look like the way he wants it to look like. So far, the volume of discussion and collaboration in this attack isn't indicating upcoming DDoS attacks, in the sense of distributing tools and lists of vulnerable sites, sites to be attacked, and compromised hosts to execute the attacks from, as we've seen it happen in Estonia's incident. It surely proves that they are motivated enough to go further.

3.5m hosts affected by the Conficker worm globally | ZDNet

A recently conducted experiment by F-Secure estimates that [approximately 3.5 million hosts have been infected](#) with [W32/Conficker.worm](#) also known as [W32.Downadup](#) spreading through the now patched [MS08-067](#) as of [November, 2008](#) . Basically, [F-Secure's experiment](#) took advantage of the very same [domain registration algorithm](#) that the cybercriminals were using in order to temporarily redirect some of the infected hosts and in the meantime count the number of infected hosts.

With several [new Conficker variants](#) released since the [original November campaign](#) , the worm's authors seem to be diversifying the propagation vectors in order to [increase the worm's lifecycle](#) .

The latest propagation tactics include USB spreading, network shares spreading, and according to McAfee, the latest samples that they've analyzed are [attempting to exploit only English language OS versions](#) thanks to an OS fingerprinting feature within a Metasploit exploit used by the worm's authors.

Ever since the first release of the worm, the authors' criminal intentions became pretty evident. Infected hosts would be exposed to fake security software claiming that the host's security has been compromised -- appreciate the irony here -- with the worm's authors earning \$30 for each and every successful sale of the bogus security software. This approach of monetizing malware infected hosts through an affiliate-based network is one of the main incentives for assembling a botnet these days.

27 of 100 tested Chrome extensions contain 51 vulnerabilities | ZDNet

[A group of security researchers](#) have analyzed 50 of the top Chrome extensions and another 50 chosen by random, and found out that 27 of the 100 extensions contain one or more vulnerabilities in their cores, for a total of 51 vulnerabilities :

We reviewed 100 Chrome extensions and found that 27 of the 100 extensions leak all of their privileges to a web or WiFi attacker. Bugs in extensions put users at risk by leaking private information (like passwords and history) to web and WiFi attackers. Web sites may be evil or contain malicious content from users or advertisers. Attackers on public WiFi networks (like in coffee shops and airports) can change all HTTP content. We'll show you how you can prevent attacks on your extension using Content Security Policy.

49 of the 51 vulnerabilities found can be patched by adapting the extensions to use one of two offered Content Security Policies (CSP).

The group is urging extension developers to use CSP directives to protect their users from the potential security consequences of core extension bugs.

24 cybercriminals arrested in 'Operation Card Shop' | ZDNet

According to a recently posted press release by the U.S Department of Justice, the FBI has arrested 24 cybercriminals part of an international law enforcement operation aiming to arrest and prosecute the users of a [sting operation called "Carder Profit" \(CarderProfit.cc\)](#).

The carding community known as "Carder Profit" was originally established by the FBI in June 2010 as an attempt to infiltrate the cyber underground, collect intelligence on the vendors and buyers, attempt to physically identify them, and prevent millions in potential financial losses.

The web site even operated with OPSEC (operational security) in mind, in an attempt to increase its perceived sophistication among the cybercrime community, namely it required multiple recommendations from already registered users in order to register a new account.

If you want to know everything you ever wanted to know about the carding market and more, consider going through the "[Exposing the Market for Stolen Credit Cards Data](#)" research published in October, 2011

Access to the web site was taken offline in May, 2012 with the idea to analyze the already gathered data. According to the press release, the operation prevented estimated potential economic losses of more than \$205 million, and led to the notification of credit card providers on the stolen 411,000 credit and debit cards.

Names of the arrested cybercriminals:

MICHAEL HOGUE - xVisceral
JARAND MOEN ROMTVEIT - zer0
MIR ISLAM - JoshTheGod
STEVEN HANSEN - theboner1
ALI HASSAN - Badoo
JOSHUA HICKS - OxideDox

MARK CAPARELLI - Cubby
SETH HARPER - Kabraxis314
CHRISTIAN CANGEPO - 404myth

Geographical distribution of the arrests: United Kingdom (6 arrests), Bosnia (2), Bulgaria (1), Norway (1), and Germany (1)

Yet another cybercrime-friendly community was targeted in the operation, although the press release is not discussing the matter. The community in question, **Fraud.su**, which currently returns an index page placed there by U.S law enforcement agencies.

The operation appears to be widespread, as the web site of the [UGNazi group](#) ([UGNAZI.com](#)) is also defaced by U.S law enforcement agencies.

What's particularly interesting is that, compared to the [DarkMarket](#) operation, [a spokesman for the U.S Attorney's office](#) insists that the "Carder Profit" FBI carding forum was not a sting operation because the agents did not initiate the criminal activity. However, that's not the case for the [DarkMarket operation](#), where agent Keith Mularski, known as "Master Splynter" at the time, engaged in cybercrime-facilitating actions in order to remain a trusted member of the community.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

2012 Olympics themed malware circulating in the wild | ZDNet

Security researchers from [TrendMicro have intercepted a currently circulating](#) 2012 Olympics themed emails containing malicious attachments.

The cybercriminals behind the campaign are enticing end and corporate users into opening the malicious Microsoft Office (.doc) attachment, which upon execution will attempt to exploit [CVE-2010-3333](#) (RTF Stack Buffer Overflow Vulnerability) and will later on drop a backdoor on the infected PCs. According to TrendMicro:

This backdoor may perform several malicious routines, including deleting and creating files and shutting down the infected system.

End and corporate users are advised to be extra vigilant for the upcoming increase of 2012 Olympics themed scams and malware-serving campaign, that will inevitably hit their Inboxes.

200,000 sites spreading web malware, China's hosting the most | ZDNet

Yesterday, [the Stopbadware.org initiative](#) released a report entitled "[May 2008 Badware Websites Report](#) " summarizing

the findings out of analyzing over 200,000 sites spreading malware. With recent data for malicious sites provided by [Google's Safe Browsing diagnostic](#) , Stopbadware.org also received responses from affected parties such as Google itself, The Planet, SoftLayer and iEurop. Here are more details on the methodology used, and who's who in hosting the most badware sites for May, 2008 :

Using data from Google's Safe Browsing initiative, StopBadware.org analyzed over 200,000 websites found to engage in badware behavior. The analysis found that over half of the sites were based on Chinese network blocks, with a small number of blocks accounting for most of the infected sites in that country. The U.S. accounted for 21% of infected sites, and these were spread across a wide range of networks. Compared to last year, the total number of sites was much higher, likely due both to increased scanning efforts by Google and to increased use of websites as a vector of malware infection. Several U.S.-based network blocks that were heavily infected last year, including that of web hosting company iPowerWeb, whose network block topped last year's list, no longer host large numbers of infected sites.

What's important to take into consideration when going through these stats, is that a great deal of networks hosting domain portfolios engaging in a countless number of malicious activities, would remain underreported due to the efforts them put into evading common detection approaches, the result of which is their current placement in the "Unknown" and "Other" categories. I was pleasantly surprised to see **SoftLayer** mentioned, in fact SoftLayer's response to the research at the first place, as if we are to play a game of associations the first things that come to my mind when I see

SoftLayer are The **Russian Business Network** , **InterCage, Inc.** , **Layered Technologies, Inc.** , **Ukrtelegroup Ltd** , **Turkey Abdallah Internet Hizmetleri** , and **Hostfresh** , ISPs providing infrastructure to malware command and control interfaces and malicious domains used in [the majority of malware embedded attacks during the entire 2007](#) , and early 2008.

The report makes an important point, namely, that compared to the previous year the total number of sites found to engage in badware activities was much bigger, mostly because of the increasing use of sites as infection vectors, but also because of Google's increased scanning efforts.

Don't forget that these are only the detected sites spreading malware, and with the ongoing efforts by malicious parties to implement evasive tactics in order to fool client side honeypots crawling their malicious sites, the number of malware spreading sites is much higher. For instance, for [the past couple of weeks](#) I've been [analyzing malicious doorways](#) which when properly analyzed redirect to over 10 to 20 different malware serving domains, and given most of them are also used as redirectors, [analyzing a single malicious doorway](#) ends up with a portfolio of over a 100 malicious domains. So what? Basically, the ongoing collaboration between blackhat search engine optimizers and malware authors, results in the malware authors getting empowered with know-how on cloaking their malicious doorways from search engine crawlers, and it's these search engine crawlers who make it possible for client side honeypots to verify whether or not a site is malicious or not. The doorway would serve legitimate content to a potentially identified search engine's crawler or even a client side honeypot, but would reveal it's real ugliness to the average Internet user.

Anyway, what's more disturbing at the bottom line - the fact that [legitimate sites are starting to host most of the web malware](#) these days, ruining the stereotype of "don't visit unknown sites or you risk getting infected with something", or the fact that we are not emphasizing on the average time it takes to shut down such a site at the first place, but are always curious where are they hosted geographically?

Consider going [through the report](#) , it's well worth it.

\$10k hacking contest announced | ZDNet

Israeli software developer Gizmox is challenging hackers to [try hacking into the company's Visual WebGui Platform](#) , by offering a \$10,000 incentive to those who manage to achieve the objectives of their contest launched at the beginning of the month. What's particularly interesting about the contest is the fact that the company is running the contest as an investigation into the identity of their secret agent, the data for whom resides on their unhackable platform.

Nothing's unhackable, the unhackable just takes a little longer.

"Gizmox, the developer of Visual WebGui open source platform, today announced a contest, sponsored by the Company, which will pay \$10,000 to anyone who can hack into its Visual WebGui Platform. The Contest will take the shape of an investigation into the identity of a secret agent. The goal of the contest is to uncover the true identity of their secret agent, code named OWL. The Contest will feature a flash movie presented within the Visual WebGui application that will contain the data necessary to uncovering the identity of the OWL. Participants will be required to provide a reproducible pathway into the Visual WebGui Pipeline (without having to penetrate any non Visual WebGui Peripherals) in order to claim the prize. The contest will begin on November 3rd and end January 30th, Participants must register to receive login information and contest details."

[Registration is open to everyone](#) , here are some of the highlights of what is considered acceptable hacking of the company's framework :

"- The game assumes that the database is safe and cannot be penetrated to; hacking the database in any level will not qualify. In addition gaining a more powerful username and password is only valid if done through Visual WebGui path and will not be a valid winner in any other case. - Assume in general, that any peripheral system and software is safe and cannot be penetrated through; in general a non-Visual WebGui layer hack-through will not be

considered a win. - Hacking through the Visual WebGui pipeline only is acceptable, meaning that using the VWG AJAX messages will qualify for winning the award. - Manipulating any client code (JS, XSLT, XML, HTML and any client resource) is permitted, in order to try and shift the system from its original security behavior. - Using any side effects or consequences of Visual WebGui code in runtime in order to hack the system is allowed, as long as the actual hack will use those side effects and consequences in order to manipulate the original server security behavior and not to penetrate any other software or infrastructure."

Offering financial incentives in the form of hacking contests or bug bounties are nothing new. For instance, in 2000 PacketStormSecurity offered \$10k reward for the winner in their "[Protecting Against the Unknown](#)" whitepaper contest, with another [\\$10k offered by iDefense](#) for a critical Microsoft vulnerability in 2006, followed by the most recent [PWN 2 OWN \\$10k reward](#) this year.

Gizmoz's contest is different in that it's indirectly advertising the "unhackability" of its products compared to enticing research into the products of other companies. Whatever their motivation, the contest is worth the try, especially when their [AJAX/Silverlight Web Applications Framework](#) can be "examined" for free.

10 things you didn't know about the Koobface gang | ZDNet

[Click here to see a gallery of Koobface pranks](#)

With [Koobface](#) continuing to spreading across Facebook by utilizing hundreds of compromised sites as infection vectors, next to using them as distributed hosting infrastructure in an attempt to undermine potential take down activities, a common misconception regarding the gang's activities shifts the attention from their true participating within the underground ecosystem.

The intensive multitasking on behalf of the Koobface gang, next to the fact that the Koobface botnet is the tip of the iceberg for their malicious operations, prompts the publishing of this top 10 things you didn't know about the Koobface gang list.

Some are funny, others are disturbing, the majority indicate a cybercrime ecosystem that actively keeps itself up-to-date with the very latest research profiling it, by reading the blogs of security vendors and researchers.

01. The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet

In September, 2009, researchers from ClickForensics established an interesting connection between the [Bahama botnet](#) -- the name comes from the 200,000 parked domain sites located in the Bahamas where they were redirecting the traffic to -- between what I refer to as my "[Ukrainian fan club](#) " due to the [offensive messages](#) they were [including](#) in the redirectors [every time I exposed](#) and shut down [one of their campaigns](#) .

[Malware samples pushed by the Koobface botnet, were modifying HOSTS file on the infected hosts](#) , in an attempt to redirect the user into a bogus Google featuring pharmaceutical ads, as well as related [cybercrime-friendly search engines in order to monetize the hijacked traffic](#) . The "Ukrainian fan club" itself, appears to be the blackhat SEO department for the Koobface gang, whose connections to the following campaigns, as well as the multiple connections linking it to

the then centralized Koobface infrastructure, resulted in the [take down of the Koobface-friendly Riccom LTD - AS29550](#) in December, 2009.

[Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign](#)

How did the gang respond? With a bold sense of humor.

02. Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video

Just when you start thinking that quality assurance is daily routine for these botnet masters, imagine my surprise when an [October, 2009 spoof of YouTube page](#) , was actually a screenshot taken by [using a trial](#) version of the HyperSnap.

The result? A *"Created with HyperSnap 6. To avoid this stamp, buy a license "* at the bottom of the screenshot, shown to everyone visiting a Koobface infected hosting serving it. The entire YouTube spoof was basically a screenshot taken from a legitimate video page, with the spoofed Adobe error message, being the only part of it that was clickable.

03. The Koobface gang was behind the malvertising attack the hit the web site of the New York Times in September

Data and real-time OSINT (open source intelligence) analysis speaks for itself. With ClickForensics [establishing a connection](#) between my "Ukrainian fan club" the Bahama botnet, and the malvertising attacks, the [assessment of the incident](#) further confirmed this connection based on historical OSINT gathered from their previous blackhat SEO campaigns.

[The Koobface/Ukrainian fan club connection?](#) The same redirector used in the [NYTimes malvertising attack](#) , was not only simultaneously found on Koobface infected hosts, but was also profiled a month earlier in the "[Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign](#) ", a blackhat SEO campaign maintained by them.

04. The gang conducted a several hours experiment in November, 2009 when for the first time ever client-side exploits were embedded on Koobface-serving compromised hosts

With Koobface representing a case-study on successful propagation across social networking sites, relying on social engineering only, in November, for the first time ever, they [conducted an experiment lasting several hours, where client-side exploit serving iFrames were embedded](#) on Koobface infected hosts.

Sampled exploits included VBS/PySme.BM; Exploit.Pidief.EX; Exploit.Win32.IMG-WMF, moreover, despite the Koobface gang's claim -- more on that claim and their bold sense of humor in an upcoming post -- on the very same IP hosting the exploit serving domain, there was an active Zeus crimeware campaign.

By embedding these particular domains, the gang also exposed an affiliation with an author of a popular web malware exploitation kit. Whether the experiment was meant to test its exploitation capabilities before the gang would start serving exploits permanently remains unknown. A few hours after their experiment was exposed, they suspended it.

05. The Koobface gang was behind the massive (1+ million affected web sites) scareware serving campaign in November, 2009

Remember the [massive blackhat SEO campaign from November, 2009](#) , where 1+ million web sites were found compromised and serving scareware?

Real-time monitoring of the campaign, and cross checking the data with real-time monitoring of Koobface activity revealed an interesting observation. The [redirectors embedded on the compromised web sites, are also the same redirectors found on Koobface infected hosts](#) , both pushing scareware.

[Are Mac OS X users left behind? -->](#)

06. The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie marketplaces

Earlier this month, upon analyzing the techniques the gang uses to efficiently compromise web sites and backdoor them, I stumbled

upon [an early stage experiment attempting to monetize Mac OS X traffic through legitimate and fraudulent dating agencies](#) .

Over the past two weeks, the gang has changed the monetization, and is now currently redirecting Mac OS X visitors to an online movie marketplace, based on whose registration details we can clearly see that the email used to register the site in question, has also been used to register dozens of scareware/fake security sites. You judge the legitimacy of the service.

This very same Mac OS X monetization attempt was also seen in a blackhat SEO campaign ([News Items Themed Blackhat SEO Campaign Still Active](#)) managed by the gang in September, 2009.

07. Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas

Throughout the entire 2009, the Koobface gang which now officially describes itself as [Ali Baba](#) following my discovery of their pseudonym on a compromised web site -- Ali baba is a fictional character from medieval Arabic literature, with Aliba Baba and 40 as the film adaptation of the "[Ali Baba and the Forty Thieves](#)" -- proved that it keeps itself up-to-date with the latest research done against it.

Around the time when the [Koobface-friendly Riccom LTD - AS29550 was taken offline](#) , the gang on purposely embedded a bold greeting on Koobface infected hosts in an attempt to legitimize its activities by stating that it is not a virus, and that they have never stolen financial data. Ironically, the gang also included a "*Wish Koobface Marry Christmas*" script, where over 10,000 people have surprisingly clicked. I wonder how many of these people inquired about a PC repair service, or filed a (scareware) fraud report once they checked their bank statements at the end of the month?

The message they included on the Koobface infected hosts is as follows:

"Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

Kaspersky Lab** for the name of Koobface and [25 millionth malicious program award](#) ; **Dancho Danchev

(<http://ddanchev.blogspot.com>) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware; **Trend Micro** (<http://trendmicro.com>), especially personal thanks to **Jonell Baltazar** , **Joey Costoya** , and **Ryan Flores** who had released [a very cool document \(with three parts!\)](#) describing all our mistakes we've ever made; **Cisco** for their 3rd place to our software in their annual ["working groups awards"](#) ; **Soren Siebert** with [his great article](#) ; Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system. By the way, we did not have a cent using Twitter's traffic. But many security issues tell the world we did.

They are wrong. As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards.

Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry. We work on it :) Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang "

Who is Soren Siebert? According to [the folks at Abuse.ch](#) , who also maintain the ZeusTracker ([Crimeware tracking service hit by a DDoS attack](#)):

On my blog you will find a reference to a disclaimer page in the navigation bar. The disclaimer is written in German and was generated with a impressum generator provided by e-recht24.de. So the Koobface gang just came across this name on my disclaimer and thought that this is my name.

08. The Koobface gang once redirected Facebook's IP space to my personal blog

In 2009, the Koobface gang had a fixation on me, which didn't come to as a surprise given the comprehensive connections that I was able to establish. That's of course next to the take down of the majority of command and control servers used in Koobface 1.0, over a period of 24/32 hours, which prompted the gang to implement their contingency plan, one they appear to have been developing for a while.

In July, 2009, I was [the only individual ever singled out](#) , with the gang leaving [the following message](#) within their [command and control infrastructure for nine days](#) :

"We express our high gratitude to Dancho Danchev (<http://ddanchev.blogspot.com>) for the help in bug fixing, researches and documentation for our software."

Pretty diplomatic way of thanking me for having them kicked out of their ISPs, and systematically suspending the domains that botnet used as foundation for propagating and communicating with the already infected hosts? Depends.

In the next few months, the gang was experimenting with various ways to show me that they're aware of my research/take down activities by typosquatting domains using my name such as **pancho-2807 .com** (registered to *Pancho Panchev*; pancho.panchev@gmail.com), followed by **rdr20090924 .info** (registered to *Vancho Vanchev*, vanchovanchev@mail.ru). Then they decided to set a new benchmark.

In September, 2009, while checking my daily stats I noticed a sudden peak of visitors. Digging a little deeper I was surprised to see that all of them were coming from within Facebook Inc's network. [What the Koobface gang did, was to basically redirect Facebook's IP space to personal blog](#) , every time a [Facebook crawler was visiting](#) their automatically [registered Blogspot accounts](#) .

Upon contacting Facebook's Security Incident Response Team, the folks implemented a filter and responded by confirming this was happening:

Thanks for bringing this to our attention. I'm on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off. All visits to Koobface URLs from our IP space are currently being redirected to your blog.

Pretty dynamic "relationship", isn't it?

09. The gang is experimenting with alternative propagation strategies, such as for instance Skype

With the [Koobface botnet under the microscope](#) of the security community, the gang is naturally interested in switching its social engineering tactics, or looking for alternative propagation methods.

In November, 2009, [security vendors detected](#) a new Koobface variant indicating their long-term strategy of diversifying the propagation vectors - [by using Skype](#) . The sample analyzed back then, was also collecting personally identifiable information from the affected users, a practice that is often used when a malicious attacker is building the foundations for a successful social engineering campaign.

Why would the gang bother propagating through Skype with such a well developed Web 2.0 propagation strategy already in place? Greed is the first thing that comes to my mind.

10. The gang is monetizing traffic through the Crusade Affiliates scareware network

Originally exposed in September, 2009's "[Koobface Botnet's Scareware Business Model](#) " post ([See Part Two as well](#)), when they officially started serving scareware each and every time a user visits a Koobface infected page, the Crusade Affiliates network appears to be primary choice for the Koobface gang in terms of scareware monetization.

Once its key domain got suspended, the network went undercover, although it appears that the entire network may be an exclusive

operation maintained by, and used only by the Koobface gang in an attempt not to attract so much attention to its activities. This operational security (OPSEC) practice on behalf of Koobface and the network has been evident ever since, with the lack of branding whereas the gang still collects the revenue from the network, which is naturally earning profit thanks to the Koobface botnet.

Scareware continues being the single most profitable monetization strategy used by the gang. The success of this business model is pretty evident with [PC repair shops noticing an increasing demand](#) for their services thanks to scareware/fake security software ([See a gallery of different scareware releases](#)) infections.

Your most pragmatic strategy when fighting scareware in general, remains [secure browsing](#) , awareness ([The ultimate guide to scareware protection](#)), or plain simple [sandboxing](#) .

\$1 Million prize offered for cracking an encryption algorithm | ZDNet

It's 2008, and companies perhaps rich on VC money to waste in a guerilla marketing tactic for generating viral buzz, still

talk and act as the [utopian "unbreakable encryption" algorithm is the panacea of security](#) , or the "[Hackers Hell: Privacy That Can't Be Compromised](#) " as they pitch it.

[Permanent Privacy](#) is one of these companies suffering from [marketing myopia](#) , and re-inventing the wheel by promotion what's already available on the market, unbreakable encryption if the algorithm is directly attacked, and the opportunity for obtaining the keys and passphrases through malware excluded. They are, whatsoever, offering \$1m to those who manage crack their data encryption system :

"Permanent Privacy announces the world's first practical data encryption system that is absolutely unbreakable. And is offering a \$1,000,000 challenge to anyone who can crack it. Permanent Privacy (patent pending) has been verified by Peter Schweitzer, one of Harvard's top cryptanalysts, and for the inevitable cynics Permanent Privacy is offering \$1,000,000 to anyone who can decipher a sample of ciphertext. Peter White, Managing Director of Permanent Privacy, said:

"The world of cryptography shuns and disparages outsiders, but Permanent Privacy is the real thing. You can now send emails and store data with 100% security. Even the Pentagon can't read your secrets if they don't have the keys".

There's a business model in here, and not necessarily the brand with a mission like you'd want it to be. For instance, in order to [participate in the challenge](#) , you'd have to purchase the tool for \$39 - "*Each licence bought will entitle one entry into the Million Dollar Challenge* ", and what follows is the best part. Even if you purchase it and encrypt a message, the [person who wants to decrypt the message would also have to purchase the tool](#) - "*if your friend*

wants to decrypt something you've sent he/she will also need to purchase PP as well. " Thinking for a second about the number of people with whom you exchange encrypted emails on a daily basis, and how they wouldn't be able to read them unless they too, purchase the tool, ruins my understanding of public key cryptography.

As far as the "unbreakable encryption" is concerned, it's already there. [The GPcode](#) authors [use it](#) , and probably you use it, which doesn't mean that you are no longer susceptible to malware and spyware attacks aiming to steal your secret keys and passphrase, since it would be virtually impossible, if not impractical to directly attack the encryption algorithm used. Cases in point :

the recent [espionage attempts against pro-tibet groups](#) were aiming to steal their PGP encryption keys through malware

[police spyware also known as fedware](#) aiming to assist law enforcement in dealing with "unbreakable encryption" is only starting to take place as a concept

in Bavaria, [Skype encryption wiretapping trojans](#) are already legally used and, of course, abused lawfully

These ongoing developments clearly indicate that whenever the algorithm cannot be cracked, adaptive approaches are already in the works, and so even the "unbreakable encryption" can be simply bypassed by stealing your keys and associated passphrase through malware. Therefore, the "unbreakable encryption" used in a compromised environment is literally worth nothing.

1.5m spam emails sent from compromised University accounts | ZDNet

With the increasingly common [spamming as a service](#) underground propositions [relying on botnets](#) , and services offering thousands of [pre-registered accounts at popular email providers](#) , it would be logical to consider that old school techniques consisting of compromising accounts and abusing them to send as many spam emails as possible in the shortest time frame achievable, have long disappeared from the arsenal of the spammer. However, there are always "amateur exceptions" proving otherwise.

By personalizing phishing emails (spear phishing) impersonating the University of Otago, spammers managed to obtain the passwords of four staff members, [whose accounts were used to send 1.5m spam emails in 60 hours](#) during the last couple of days.

"Hackers gained access to the University of Otago staff email server recently and used it to send out an estimated 1.55 million spam emails in 60 hours, after tricking four staff members into revealing their login details. The huge volume of spam mail resulted in legitimate emails being rejected or delayed by other systems, information services manager Mike Harte said. They were re-sent once the spam attack was over. The staff members responded to "spear phish" emails which claimed to be from the IT department and asked people to reconfirm their user names and passwords or their email access would be withdrawn."

The spammers didn't just abuse the clean IP reputation of the University, they also had its mail servers blacklisted thereby causing a DoS attack to its staff and students. The [University's official notice of the incident](#) :

"The university is currently experiencing access and delivery issues with Stonebow webmail. A number of Stonebow accounts have been compromised by staff members responding to a phishing email. These accounts have been used to distribute spam. This has resulted in the university mail server being blacklisted by a number

of providers. ITS has disabled those accounts affected and temporarily disabled off campus access to Stonebow webmail as the spammers are actively moving from one account to another. ITS is working to get the university removed from the blacklists.

ITS will monitor service providers that do not accept email from Otago and work with them to re-establish email services in the coming few days. If any administrators are in contact with staff currently overseas, please advise them of the current email situation."

Theoretically, the tools and the motivation to abuse the access to compromised accounts have always been there, but such attempts are more of a fad rather than a trend, since these days spammers are actively outsourcing the entire process of botnet creation and supply of new bots with clean IP reputations to malware authors. How come? It's far more cost-effective than having to do it on their own.

[Image courtesy of Modern Life](#) .

1.5 million Facebook accounts offered for sale - FAQ | ZDNet

In their latest "Weekly Threat report", [VeriSign's iDefense Intelligence Operations Team](#) has profiled the underground market proposition of someone claiming to have 1.5 million compromised Facebook accounts available for sale.

The pricing method is based on the number of contacts per compromised account, presumably with the idea to allow easier spreading of related malicious content across Facebook.

Here's an excerpt from the report, and a brief FAQ on the underground ad.

"On Feb. 10, 2010, (cybercriminal) stated that he or she is selling 1.5 million compromised Facebook accounts, in bulk quantities, belonging to users in various countries. The price per 1,000 accounts varies based upon the number of friends and contacts that each account possesses. For a purchase of compromised accounts containing 10 contacts or fewer, a buyer must pay \$25 per 1,000 accounts. A purchase of compromised accounts containing 10 or more contacts requires a buyer to pay \$45 per 1,000 accounts. Accounts containing zero contacts are also available for bulk purchasing from (cybercriminal), at the cost of \$15 per 1,000 accounts. The prices of these accounts are presumably in USD or the equivalent amount in some form of electronic currency."

Sometimes, there's no honor among cybercriminals ([Phishers increasingly scamming other phishers](#)), just like there isn't among "real life" thieves.

From the distribution of backdoored web interfaces to web malware exploitation kits, to the actual "binding" of additional malware to the original release, sophisticated or at least cybercriminals with experience, have realized that there are thousands of potential cybercriminals that could unknowingly start working for them. The process of *"cybercriminals attempting to scam*

novice cybercriminals " demonstrates just how vibrant the ecosystem has become these days.

With a huge percentage of the underground marketplace driven by reputation, this is exactly what this particular seller of Facebook data is missing. Moreover, with quality assurance now an inseparable part of the cybercrime ecosystem, the seller is not just skipping the time frame in between which the accounts were compromised, he is also not mentioning have many of them are actually verified as working.

These, and several other factors make me skeptical on the quality of this underground proposition.

If we consider that the cybercriminal's claims to be true, how did he manage to obtain 1.5 million Facebook accounts?

The ad is clearly stating that they are accounts with contacts, meaning they're compromised, and other which have zero contacts, meaning they've been automatically generated by outsourcing the CAPTCHA-solving process to international teams specializing in the process.

Related posts: [Inside India's CAPTCHA Solving Economy](#); [Report: Google's reCAPTCHA flawed](#) -- 1 million solved reCAPTCHAs for \$800 through outsourcing

The compromised accounts could have been obtained through the emerging [Cybercrime-as-a-Service \(CaaS\) market model](#). For instance, if he has paid \$100 for 3GB of raw crimeware data, and the data mining allowed him to compile a list of 1.5m Facebook accounts, based on the current price, he'll [automatically break-even](#).

Phishing campaigns shouldn't be excluded as a possibility, however, it remains unclear whether the seller has launched them personally, or managed to purchase the raw data from someone else.

What kind of a business model within the cybercrime ecosystem would allow him to sell the data so cheaply, and still make a profit?

It's a business model with an ever-decreasing cost of supply, based on the currently active "*malicious economies of scale* "

phrase. This efficiency-driven cybercrime model is in fact so successful, that whether consciously or subconsciously, cybercriminals are realizing the [basics of market liquidity](#), and the [time value of "underground goods"](#), in particular the decreasing future value of assets like the Facebook accounts -- the value becomes zero when the affected user changes his password from a malware-free host.

Related posts: [Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime](#) ; [Report: Malicious PDF files comprised 80 percent of all exploits for 2009](#) ; [Microsoft study debunks phishing profitability](#) ; [Microsoft study debunks profitability of the underground economy](#).

Why would a cybercriminal want access to your Facebook account?

For a variety of fraudulent reasons, all of them exploiting the already established trust relationship between the compromised account's holder and his network of friends.

From "[money transfer schemes](#) " where the fraudster is supposedly stuck somewhere and requires cash, to a malware campaign relying on nothing else but a status message leading to a client-side exploits serving site. Your network of friends, turns into his network for propagation of fraudulent/malicious schemes and campaigns.

[VeriSign's iDefense](#) also makes an interesting observation.

With Facebook's user base growing to 300 million people across the globe, this indispensable marketing platform can be easily integrated into the cybercriminal's arsenal, with localized and targeted social engineering attacks relying on basic market segmentation, launched with the idea to achieve a higher conversion rate, compared to mass marketing approaches.

Fact or fiction, based on the ad's content, this is perhaps **the perfect time to change your Facebook password from a malware-free host** , since a strong password is just as weak as the weak one in general if there's malicious code present on the system.

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/> and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back these settings

CLOSE

Cybercriminals release Christmas themed web malware exploitation kit | ZDNet

"Committing cybercrime around the Christmas tree" has always been a tradition for malicious attackers introducing new ways to scam the millions of online shoppers during the holidays. This Christmas isn't going to be an exception, but what has changed compared last couple of years is the tone of the Xmas promotions already circulating across various cybercrime communities. Do cybercriminals exchange gifts during the Christmas holidays? A recently released [web malware exploitation kit](#) coming with three different types of licenses and 9 modified exploits, aims to become "the perfect Christmas gift for all of your friends".

Not surprisingly, the exploitation kit itself is released purely for commercial gains which when combined with the fact that it appears to be using a large percentage of the source code from a competing exploitation kit -- appreciate the irony here -- the already patched vulnerabilities it attempts to exploit can be easily taken care of. However, going through the infection rate statistics which were temporarily left available as a promotion tool, thousands of people have already become victim of their lack of decent situational awareness on how important patching of their third-party applications really is.

A translated description of the kit's marketing pitch :

"Feeling bored? Miss the Christmas spirit? Want to make a lot of money before the holidays but you lack the right tools? We have the solution to your problems - our web malware exploitation kit which will bring back the Christmas attitude and also become the perfect gift for your friends. Available are Professional, Standard and Basic licenses, with each of these including or lacking some unique features based on your budget. Professional package comes with support."

Modified exploits included within with their associated descriptions :

modified MDAC - "the notorious exploit that continues to provide high infection rates of IE6 users"

IE Snapshot - "unique exploit offering high infection rates for both IE6 and IE7 users"

FF Embed - "still relevant for exploiting all Firefox versions"

Opera Old+new - "capable of infecting all versions of Opera up to the latest one"

Old PDF - "targeting Adobe Reader v8.1.1 it's still relevant, also it checks whether the exact version is installed before launching the exploit"

New PDF - "targeting Adobe Reader 8.1.2, a perfect combination with Old PDF"

XLS - "unique exploit targeting Microsoft Excel"

SWF- "modification of the infamous exploit, works quietly and targets all browsers"

The malware obtained in one of the currently active campaigns has a low detection rate (6 out of 37 AVs detect it - 16.22%) and continues phoning back home to **findzproportal1.com** (64.69.33.138; 72.233.114.126) from where it attempts to drop a rootkit (**TDSSserv.sys**). Among the main ways of ensuring that you're going to ruin their holidays is to make sure they're not exploiting you with last year's client-side vulnerabilities, which is the main vehicle for continuing growth of web malware exploitation kits in general.

Cybercriminals promoting malware-friendly search engines | ZDNet

The cybercriminals behind the ongoing blackhat search engine optimization attacks hijacking swine flu related queries in order to serve scareware, have re-introduced an old social engineering tactic - the use of fake and malware friendly search engines.

[Researchers from PandaLabs](#) have recently uncovered a similar malicious search engine part of the blackhat SEO campaign, where the majority of searches lead to malware serving sites.

Three of the legitimately looking search engines have been in operation since January, 2009, [and are operated](#) by the same [group of cybercriminals](#) whose [blackhat search engine optimization practices](#) are so successful, that according to publicly obtainable traffic data two of the sites have already passed the 250,000 unique visitors benchmark in March, 2009.

The first one has approximately 257,512 unique visitors +63.64% increase since last month, followed by the second one which has approximately 279,665 unique visitors with a +64.26% increase since last month, and the third one is apparently lacking behind with 39,175 unique visitors, a +22.63% increase since last month.

Where is all that traffic coming from? 60.08% of the traffic to the first one came from Google, 12.87% of the traffic to the second one came from Google, and 26.55% of the traffic to the third one also came from Google. Google is appearing on the top of the their (approximate) traffic referrers due to the active blackhat SEO campaigns hijacking traffic from the search engine.

Go through related posts: [Inside an affiliate spam program for pharmaceuticals](#) ; [Cybercriminals syndicating Google Trends keywords to serve malware](#) ; [Google Video search results poisoned to serve malware](#) ; [Malware-infected WinRAR distributed through Google AdWords](#)

Interestingly, the search engines themselves are not visible in Google's results, an evasive practice applied by the cybercriminals

who only serve malicious content to users visiting their sites upon clicking on a link from a pre-defined search engine where the blackhat SEO campaigns are active, in this case - Google, MSN, Yahoo, Comcast and AOL.

Upon following a sample link from the phony search engines, we're redirected to domains operated by services that have been in the cybercrime-facilitating neighborhood for years, on further redirect to scareware ([Trustedwebsecurity](#) ; [Spyware Cease](#)) and online casino scams. From instance, **searchadv.com** , which was [serving WMF \(Windows Metafile\) exploits in 2006](#) to users searching through it, and **7search.com** , a Pay Per Click Search Engine Advertising network :

"7Search.com has been a leading Pay Per Click Search Engine Advertising and Affiliate Network since our inception in 1999. As a Search Engine who is dedicated to value and service for online businesses, 7search.com provides thousands of Web entrepreneurs with an economical and measurable opportunity to obtain Internet traffic and generate revenue through their online presence."

The company [sued McAfee in 2008 for labeling it as a spyware and potentially dangerous site](#) , which isn't the first, and definitely not the last time when [affiliate networks attempts a frontal attack](#) against vendors/researchers.

The use of these fake and malware-friendly search engines demonstrates the complexities of the cybercrime ecosystem, due to the double-monetization approach applied by the cybercriminals, earning pay per click revenue from the affiliate networks, and earning more revenue from serving search results serving scareware and pharmaceuticals with their own affiliate code.

Cybercriminals offer bogus fraud insurance services | ZDNet

Security researchers from [Trusteer have spotted a clever new technique](#) used by cybercriminals interested in optimizing their malicious campaigns in an attempt to earn more revenue.

Here's how it works:

The recent attack we discovered uses the Tatanga malware platform. In the configuration file we captured, Tatanga notifies the online banking victim via a web browser injection that their bank is offering free insurance protection against online fraud. The victim is then presented with a fake insurance account that claims to cover the total amount of funds in their bank account. This fake insurance account is actually a real bank account that belongs to a money mule. The victim is told that they will be protected against any losses from online fraud by this insurance coverage. In the final step, the victim is prompted to authorize a transaction that they believe is to activate the insurance coverage. In all likelihood, the victim does not expect any funds will be transferred out of their account. To approve the transaction the victim enters a one-time SMS password that is sent to their mobile device. Unfortunately, the victim is actually approving a transfer of funds from their account to the fraudster's money mule account.

Despite the technological implementation behind the success of the campaign relies on the Tatanga malware platform, a central role for the success of the concept is played by [money mules](#).

Recruited through bogus 'work at home' job offers offering up to 45% revenue sharing schemes for amounts starting from \$5000 and going up to \$7000, thousands of average Internet users unknowingly become active participants in the cybercrime ecosystem. The process, now largely standardized, relies on bogus companies set up for the purpose of recruiting unaware Internet users into processing fraudulently obtained funds.

Trusteer's latest discovery is another indication that the cybercrime ecosystem isn't short on creative and new techniques to optimize hosts that are already infected with malware.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Cybercriminals impersonate popular security vendors, serve malware | ZDNet

Security researchers from [Websense have intercepted](#) a currently circulating spam campaign, impersonating popular antivirus vendors in an attempt to trick end and corporate users into downloading and executing the malicious attachment.

According to Websense, the campaign is low-volume, and is currently impersonating Symantec, F-Secure, Verisign and Sophos.

The malicious payload ([MD5: ebb4ac5bb30b93e38a02683e3e7c98c6](#)) is currently detected by 3 out of 42 antivirus scanners as Trojan.Agent/Gen-Banload; TROJ_GEN.R47H1HR.

Upon successful execution, the sample phones back to [hxxp://bluemountain-ecards.net/images/loader.php](http://bluemountain-ecards.net/images/loader.php) (69.73.138.167), [hxxp://asselegis.org.br/images/txt.txt](http://asselegis.org.br/images/txt.txt) (187.73.33.54), [hxxp://basketcoach.com/images/logos/Plugin.dll](http://basketcoach.com/images/logos/Plugin.dll) (94.23.235.157).

Users are advised to avoid interacting with the emails, and to consider reporting them as spam as soon as they come across them.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Cybercriminals hijack Twitter trending topics to serve malware | ZDNet

A currently ongoing malware serving campaign across Twitter, is continuing to [abuse the momentum offered by Twitter's](#) trending topics in order to trick users into visiting bogus exclusive video sites and infect them with malware.

The campaign, [spreading since last week](#), is relying on a growing number of [automatically registered bogus Twitter accounts](#), which [combine trending topics and hashtags](#) with custom messages and pre-defined Tinyurl links, all leading to identical fake codec which is dropping three different malware samples.

Let's dissect their activities, and find a common pattern of exploitation.

This very latest campaign once again demonstrates that [malicious parties do not maintain a static list](#) of potentially dangerous keywords, in fact, thanks to the dynamic nature of today's Web, they serve malware in real-time by [automatically syndicating the Web's buzz and mixing it with malicious content](#) hosted on legitimate services whose high pageranks ensure the lowest possible time frame for having their content crawled by public search engines.

What has changed since last week is the intensity of the campaign, which now includes many new topics, which the bogus accounts advertise with over 150 tweets on average during a period of 24 hours.

The tweets are generated by using popular hashtag or Trending topics combined with their campaign message and a relatively static Tinyurl link.

Here are some of the topics currently used in the campaign:

Shocking video today, Headline news video, Shocking news theme

Airplane crashes theme, for instance, Jumbo Jet 747 on fire, 280 deaths, Little Cessna crash in Vancouver, Airbus A330-200 Crash

Video, Young childred killed in car crash, Terrible car crash in Fresno, CA, 15 deaths, online video, Airbus A330-200 Crash Video, AA AIRBUS A340 CRASH in Auburn, 189 fatalities

Celebrities in front of shopping mall theme

Rape theme - Raped Tonight by 20 skinheads - HEADLINE News Video, Pedophile raped over 580 children, Rihanna Raped Tonight by 20 skinheads in Maryland State. VIDEO

Upon following any of the links, the users are redirected to a Mal/FakeAV-AY ([streamviewer.40030.exe](#)) serving site attempting to trick the visitors with a common social engineering theme, the lack of required codec in order to view the video.

Cybercriminals adapt pretty fast, for instance, last week's campaign was using the **bit.ly** URL-shortening service which does cross-check submitted URLs for possible maliciousness using community-driven databases.

The effectiveness of this common sense technique is best described with the "*Warning - this site has been flagged by SURBL and may contain unsolicited content.*" message served for the very same domain that the malicious parties are now freely redirecting to through **TinyURL**.

Cybercriminals hijack Facebook accounts through bogus browser extensions | ZDNet

[Researchers from WebSense](#) are warning on a newly circulating fraudulent scheme relying on bogus browser extensions for hijacking Facebook accounts.

The add-ons, advertised as DivX plug-ins or coupon generator, use the Facebook API (Application Programming Interface) to post unauthorized messages on behalf of Facebook users who log in from the affected browsers.

According to the researchers, at the moment, only Chrome and Firefox plugins are used.

Cybercriminals exploiting the death of Kim Jong-Il | ZDNet

[Security researchers from TrendMicro](#), have intercepted a currently circulating malware campaign, using the death of Kim Jong-Il as a social engineering heme.

The messages arrive with a .PDF attachment that has the file name **brief_introduction_of_kim-jong-il.pdf.pdf** . Upon execution, the sample drops a malicious file detected as [BKDR_FYNLOS.A](#) . The backdoor connects to its C&C server to receive and execute commands such as downloading,uploading, and executing of files, terminating processes, and performing shell commands.

The sample also exploits the following Adobe Reader and Acrobat vulnerabilities - [CVE-2010-2883](#) ; [CVE 2011-0611](#).

Users are advised to ensure that they are free of client-side vulnerabilities found in third-party applications and browser plugins, as well as to exercise extra caution when opening attachments coming from unknown sources.

Cybercrime friendly EstDomains loses ICANN registrar accreditation | ZDNet

Despite [EstDomains](#) persistent [press releases](#) during the last [couple of days](#) , next to the domain registrar's [delayed response to the security community](#) , on Thursday the ICANN has sent [a notice of termination of their registrar accreditation agreement](#) with EstDomains, following obtained court records stating that [EstDomains president Vladimir Tsastsin](#) has been convicted of credit card fraud, money laundering and document forgery on 6 February 2008. [The end of EstDomains?](#) Could be, but their malicious customers are not going offline anytime soon.

"On 28 October 2008, ICANN sent a notice of termination to EstDomains. Based on an Estonian Court record, ICANN has reason to believe that the president of EstDomains, Vladimir Tsastsin, was convicted of credit card fraud, money laundering and document forgery on 6 February 2008. ICANN received a response from EstDomains regarding the notice of termination. To assess the merits of the claims made in EstDomains' response, ICANN has stayed the termination process as ICANN analyzes these claims. ICANN's records indicate that EstDomains has approximately 281,000 domain names under its management. ICANN will take all reasonable measures to protect the interests of registrants during the stay period and the subsequent termination process that may follow."

On 29 October 2008, EstDomains' Konstantin Poltev responded to the ICANN, with documents claiming that their convicted CEO has resigned in June 2008, but that EstDomains didn't notify ICANN of the change. Is he buying time, or is he making a point? Whatever the case, taking into consideration the fact that EstDomains manages over 280,000 domains, the ICANN is already soliciting requests for [bulk transfer of EstDomains portfolio to another domain registrar](#) :

"As the result of the de-accreditation of EstDomains, Inc. (IANA ID 832), ICANN is seeking Statements of Interest from ICANN-

accredited registrars that are interested in assuming sponsorship of the gTLD names that had been managed by EstDomains."

With the ICANN interested in *"taking all reasonable measures to protect the interests of registrants during the stay period and the subsequent termination process that may follow"*, among these very same registrants are the malicious cybercriminals whose portfolios of domains will be basically transferred to another registrar. Moreover, with the increasing number of domain registrars offering [bulk domain registration services](#), cybercriminals could easily damage the reputation of legitimate registrars by simply starting to take advantage of their services.

Disconnected from the Internet at the end of September, [Atrivo/Intercage's marginal thinking](#) approach of being [always on the run](#), yet managing to satisfy the uptime needs of their malicious customers, is similar to what EstDomains rogue customers will be dealing with for months to come - increasing the average online time for their malicious domains with their cybercrime friendly registrar no longer in business.

Cyber terrorists to face death penalty in Pakistan | ZDNet

According to a recently signed "[Prevention of Electronic Crimes Ordinance 2008](#)" in Pakistan, any person who commits cyberterrorism causing the death of other people will face death penalty or life imprisonment :

"Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life, and with fine and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees, or with both."

With cyber terrorism remaining an open topic term that could be greatly abused or wrongly interpreted, it's interesting to see how a country with [3.5M Internet users reported in 2007](#) defines the term cyberterrorist, and is general cybecrime treated appropriately.

"For the purposes of this section the expression "terroristic act" includes, but is not limited to,- **(a)** altering by addition, deletion, or change or attempting to alter information. that may result in the imminent injury, sickness, or death to any segment of the population; **(b)** transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity; **(c)** aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed; **(d)** stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction."

Guess what - each of these points excluding **(a)** and **(d)** can be abused and wrongly interpreted as a act of cyber terrorism. Under **(b)** fall all the script kiddies that have been defacing web sites of the

Pakistan Government throughout 2008, which according to [Zone-h.org](#) there have been a total of 201 attacks of which 132 single ip and 69 mass defacements. The harmful program in this case would be the DIY SQL injectors, the web site defacement tools, and web web shells uploaded in order for the defacers to start hosting malicious content at the compromised sites. Moreover, "any public entity" can be interpreted in a way that can easily put the [ASProx botnet](#) campaigners on a death row. In regard to (c) aiding the conspiring process against the Government can be forwarded to people who have absolutely no idea that [their Internet connectivity is abused in such a way](#) .

The ordinance is also covering other cybercriminal activities in detail, with cyber stalkers getting the maximum possible sentence, and spammers the minimum one :

Misuse of encryption in order to prevent local enforcement from gathering evidence - five years in jail, fine, or both

Malware coding - five years in jail, fine or both

Cyber stalking - seven years in jail, fine or both

Spamming - fines and up to three months in jail

Spoofing or impersonation - three years in jail, fines or both

Naturally, local organizations such as the The National Commission for Justice and Peace (NCJP) of the Catholic Church and the Human Rights Commission of Pakistan (HRCP) [are criticizing the signed order](#) :

"The secretary of the NCJP, Peter Jacob (in the photo), tells AsiaNews: "We are surprised and shocked that the government has added death penalty in cyber crimes ordinance. This is not the right way to stop the crimes. Severe punishments can not correct or mend our society. So, NCJP demands that death penalty should be immediately excluded from the list of punishments." "We are unable to understand the mentality and strategy of the government that what it wants to do. First they condemn death penalty and sign UN human rights instruments and then they impose death penalty without consulting the parliament." For the secretary of the NCJP, the imposition of the ordinance without discussion in the assembly is

"illogical" and contradicts "the statements of the government about the supremacy of parliament."

The bottom line - given the open topic definition of what constitutes an act of cyberterrorism, especially when the suspect is facing a death penalty, the ordinance seems to be more of a self-regulation awareness campaign courtesy of the Government of Pakistan.

Cutwail botnet spamming 'IRS unreported income' themed malware | ZDNet

Researchers from MX Logic -- now part of [McAfee](#) -- have intercepted [a new malware campaign spammed](#) by the [Pushdo/Cutwail botnet](#) , that's using an '*IRS unreported income*' notices in an attempt to trick the recipients into downloading a [tax-statement.exe](#) executable.

The Pushdo/Cutwail botnet remains among the most aggressively spamming [cybercrime platforms](#) , with the latest campaign traffic averaging about 90,000 emails per hour according to the company.

The latest campaign is dynamically including the recipient's email within the page, as well as the user name within the executable link in an attempt to establish authenticity, using the following URL structure - **irs.gov.hyu11hep**.eu /fraud_application/directory/statement.php. Upon execution, the executable (Trojan-Spy.Win32.Zbot.gen) downloads more malicious content from known crimeware [command and control servers](#) .

Pushdo/Cutwail was among the botnets whose operations were briefly disrupted in June, 2009's [shutdown of the rogue ISP 3FN/Pricewert](#) , resulting in a short-lived 15% drop in spam volume coming from it.

Cutwail botnet resurrects, launches massive malware campaigns using HTML attachments | ZDNet

Security researchers from M86Security, are contributing the [increase in malicious malware campaigns using HTML attachments](#), to the resurrection of the Cutwail botnet, responsible for spamvertising these campaigns.

Using the company's sensor networks, the researchers observed three peaks of spamvertised malicious campaigns using HTML attachments for serving client-side exploits to unsuspecting the vulnerable users.

The campaigns in question:

The FDIC "Suspended bank account" spam campaign
The "End of August Statement" spam campaign
and the "Xerox Scan" spam campaign

Once the user downloads and views the malicious HTML attachment, JavaScript will unknowingly redirect him to client-side exploiting URL part of the cybercriminal's malicious network, that's currently relying on the Phoenix web malware exploitation kit.

More details:

The landing page that contains the exploit code is a kit used by cybercriminals particularly for this spam campaign, the Phoenix Exploit kit. This exploit kit is readily available for cybercriminals to buy and use, all they need is their own webserver that can run PHP server scripts. The image shown below is the screenshot of the actual server's "Phoenix Exploit's Kit" admin page. The "—" referrer in the statistics suggests that most visitors were NOT coming from another website but from the HTML files that the cybercriminals spammed out. It also shows over 4000 visitors, 15% of whom were successfully exploited.

Once the researchers obtained access to the command and control interface of the exploit kit, they noticed that the majority of

referrers were coming from "blank" referrer, meaning that these are end and corporate users who are downloading and viewing the malicious attachments on their PCs.

End users are advise to avoid interacting with emails used in these spam campaigns, as well as to ensure that they're not running [outdated versions of third-party software](#) running on their PCs, as well as their [browser plugins](#).

Cuil's stance on privacy - "We have no idea who you are" | ZDNet

The less popular search engines always have [the best privacy policies](#) , it's a fact. Take [Cuil](#) , the recently launched search engine pitching itself as the most comprehensive index of the Web, and their stance on privacy. [The privacy policy](#) may in fact be a privacy watchdog's fantasy come true, if we exclude [the lack of P3P compliance](#) of course :

"Privacy is a hot topic these days, and we want you to feel totally comfortable using our service, so our privacy policy is very simple: **when you search with Cuil, we do not collect any personally identifiable information, period. We have no idea who sends queries: not by name, not by IP address, and not by cookies (more on this later).** Your search history is your business, not ours. We do not keep logs of our users' search activity. We do not record the information in your cookies on our servers; your browser sends your preferences to us with each search request. This way, we do not store any personal information about you on our servers."

No matter how good it sounds, it's [violating each and every data retention policy](#) there is, that's for sure.

Such marketable statements aiming to increase the "heart share" of their potential users may in fact be untrue, and the only reason why you're not going to see their privacy policy changing anytime soon is due to the fact I doubt they would turn into a household brand that easily, thereby attracting the necessary attention to their privacy practices.

Another example of a realistic marketing strategy sticking to data retention practices, of course, the details of which can be found hidden in their FAQ, is [Ask.com's AskEraser exceptions rule](#) , another not so popular search engine. And while they make it look like the user is in control of their privacy, their exceptions totally undermine the idea :

Is there any reason Ask.com will stop deleting my search activity? Even when AskEraser is enabled, Ask.com may temporarily retain your search activity data in certain situations:

- Legal obligations -- Ask.com must abide by federal, state, and local laws and regulations. **Even when AskEraser is enabled, we may store your search activity data if requested to do so by law enforcement or other governmental authority.** In such cases, we may retain your search data even if AskEraser appears to be turned on.

No matter the privacy policy and the marketable tools "putting you in control", [what you see is not what you get](#) .

Cryptome.org hacked, serving client-side exploits | ZDNet

The popular whistle-blowing web site [Cryptome.org](#), was recently hacked, and a malicious script was embedded on it pointing to a BlackHole web malware exploitation kit.

The BlackHole Web malware exploitation kit was serving client-side vulnerabilities from **hxxp://65.75.137.243/Home/index.php** with the IP currently offline.

Apparently, the attack was configured to only exploit users running Microsoft's Internet Explorer, compared to a situation where the cybercriminals could have utilized BlackHole's true multi-browser exploitation potential, and target multiple browsers.

According to Cryptome.org's most recent note:

14 February 2012. 16:30GMT: Cryptome 100% restored with clean files. The Blackhole malware was removed on 12 February 2012. Apparently, according to the malware, only users of MS IE were targeted, bad enough.

Users are advised to ensure that they're not running [vulnerable third-party applications](#), and [browser plugins](#).

Crimeware tracking service hit by a DDoS attack | ZDNet

A week after a [newly launched crimeware tracking service](#) went public, cybercriminals didn't hesitate to prove its usefulness by [launching a distributed denial of service attack \(DDoS\) against it](#). According to the Swiss security blog, the Zeus tracker came under attack from a previously known source that also attacked **abuse.ch** over an year ago taking advantage of a well known do-it-yourself DDoS malware.

Just like November 2008's [DDoS attack against the anti-fraud site Bobbear.co.uk](#) -- with evidence that the attack was commissioned [provided by Zero Day](#) back then -- the single most evident proof of the usefulness of your cybercrime tracking service always comes in the form of a direct attack against its availability.

What is [the Zeus Tracker](#) anyway, and why is it so special at the first place?

The Zeus Tracker is a full-disclosure project keeping track of known Zeus hosting locations, [one of the most ubiquitous crimeware applications](#) cybercriminals take advantage of for years. Moreover, by maintaining [a real-time blocklist](#) that allows the community to easily take action against known Zeus domains/IPs it shouldn't come as a surprise that the service is getting attacked - simply because it exposes active crimeware campaigns.

Go through more recent DDoS attacks coverage - [GoDaddy hit by a DDoS attack](#) ; [AlertPay hit by a large scale DDoS attack](#) ; [BBC hit by a DDoS attack](#) ; [Anti fraud site hit by a DDoS attack](#) ; [Norwegian BitTorrent tracker under DDoS attack](#) ; [Georgia President's web site under DDoS attack from Russian hackers](#)

Once available as a proprietary crimeware tool costing several thousands dollars, today, pirated copies of Zeus are so prevalent, that most of the innovations attempting to improve its usefulness and abilities to sniff E-banking transaction data come from third parties in a true open source crimeware fashion. In fact, the Zeus

crimeware is so popular that cybercriminals themselves are looking for and successfully finding [remotely exploitable vulnerabilities within the kit](#) in an attempt to hijack someone else's botnet.

Moreover, with or without the Zeus Tracker's real-time data, the Zeus malware is prone to continue dominating the crimeware landscape due to its maturity into a [cybercrime-as-a-service proposition](#). For instance, the increasing number of services offering managed Zeus botnets not only allow less sophisticated cybercriminals easy access to hundreds of thousands of banker malware infected hosts, but also, the relatively low prices the services charge due to the fact that they're running pirated copies of Zeus ultimately results in the scalability of cybercrime in general.

Attempting to undermine this scalability would mean coming up with ways to shorten the average time a Zeus command and control domain/IP remains online, next to communicating the already known locations as a public service just like [the Zeus Tracker](#) does.

Credit card fraudsters sentenced in the U.K | ZDNet

U.K's SOCA (Serious Organised Crime Agency) is reporting on [the arrest of two credit card fraudsters](#) who have facilitated fraud valued at more than £26.9m by offering one-stop-shop for accepting bulk orders of stolen credit card details.

More details:

Two cyber criminals who provided a range of services to credit card fraudsters have been sentenced to almost 5 years after facilitating fraud valued at more than £26.9m. **Jay Moore**, who used the online moniker of 't0pp8uzz', set up the 'Freshshop' website to facilitate the bulk sale of stolen financial data. He recruited **Damian Horne**, known by the online moniker of 'GM', to assist in his online criminality. Moore and Horne, who met through an online 'hackers' chat forum commenced their criminal activities by selling stolen iTunes vouchers and other online gaming codes on ebay.

[t0pp8uzz](#) is also known to have discovered a variety of exploits, according to the Exploit Database. His Freshshop web site was also taking advantage of an affiliate model and was sharing revenue with cybercriminals bringing in new customers.

Upon closer examination of files found on his PCs, law enforcement agents estimate that he had access to the credit card details of 340,000 individuals. He was using the stolen funds to purchase a top of the range BMW motor car and personalised registration plate which alone was valued at over £10,000. He used a fake web design business to cover his fraudulent activities.

In total, he had £170,000 credited to his bank account and £80,700 in a safe at his home in Cromhall, Gloucestershire.

Security tip : if you want to get an in depth overview of the market for stolen credit card data, consider going through this research published in October, 2011 - "[Exposing the Market for Stolen Credit Cards Data](#) "

In April, SOCA in cooperation with the FBI, seized 36 [credit card stores offering access to stolen financial data](#), with the potential international fraud prevented by the operation estimated at being in excess of £500 million.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Copyright violation alert ransomware in the wild | ZDNet

UPDATED: Wednesday, April 28, 2010: [How to remove the ICPP Copyright Violation Alert ransomware](#)

A currently ongoing [ransomware](#) campaign is using a novel approach to [extort money from end users whose PCs have been locked down](#).

By pretending to be the fake ICPP Foundation ([icpp-online.com](#)), the ransomware locks down the user's desktop issuing a *"Copyright violation: copyrighted content detected"* message, which lists torrent files found on the infected PC, and forces the user to pay \$400 for the copyright holder's fine, emphasizing on the fact that "the maximum penalties can be five years in prison and up to \$250,000 in fines.

More details on the campaign:

Upon execution the ransomware will change the Desktop's wallpaper to the "Warning! Piracy detected!" background.

Consider going through the [The Ultimate Guide to Scareware Protection](#) to find out more about how malware/scareware and ransomware propagates, and how to avoid falling victim into the scam

It will then make sure the warnings appear every time the end user restarts PCs. In between, it will lock down the end user's Desktop, featuring the *"Copyright violation: copyrighted content detected"* window:

The window attempts to trick the end user into believing that:

"Windows has detected that you are using content that was downloaded in violation of the copyright of its respective owners. Please read the following bulletin and try solving the problem in one of the recommended ways. During the system scan Antipiracy foundation scanner has detected copyright issues. Please take a

look at the list and choose an action: pass the case to a court or settle it in pre-trial order by paying a fine. "

Attempts to get rid of it result in the following message:

"Performing this action is construed as refusal to cooperate with the copyright holder and unwillingness to consider pre-trial settlement. If you continue, all the data gathered will be passes to copyright protection organizations and to the court. We recommend cancelling this action and choosing the option "pre-trial settlement". "

Gullible end users who fall victim to the scam, will then be asked to pay \$399.85 for a "Legal license purchase ", "Copyright holder fine ", a "Copyright protection organization fee for the use of software tracking illegal file downloads " and a "Traffic fee ".

Basically, you've got a profit margin driven ransomware business model, that's ironically charging you a fee for the development of ransomware "software" itself. The cybercriminals behind the campaign are also aware of the concept of localization. The ransomware will adapt to each user's PC, and issue the same messages in 10 different languages - *Czech, Danish, Dutch, English, French, German, Italian, Portuguese, Slovak and Spanish* .

UPDATED: Find out more about this campaign's [connections with related ZeuS crimeware, and money mule recruitment campaigns](#)

Although the ransomware tactic of using copyright infringement themes is novel, the tactic is fundamentally flawed due to a simple reason - the amount of money the ransomware is requesting is supposed to trigger a "vigilance alert" in the mind of the affected user.

UPDATED2: Basic [malware/scareware/ransomware prevention tips for Windows users](#) .

The ransomware is currently detected as [Win32/Adware.Antipiracy](#) and [Rogue:W32/DotTorrent.A](#) .

Coordinated Russia vs Georgia cyber attack in progress | ZDNet

In the wake of the [Russian-Georgian conflict](#) , a week worth of speculations around Russian Internet forums have finally

materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with [Georgia's Ministry of Foreign Affairs](#) undertaking a desperate step in order to disseminate real-time information by moving to a Blogspot account.

Who's behind it? The infamous Russian Business Network, or literally every Russian supporting Russia's actions? How coordinated and planned is the cyber attack? And do we actually have a relatively decent example of cyber warfare combining PSYOPs (psychological operations) and self-mobilization of the local Internet users by spreading "*For our motherland, brothers!* " or "*Your country is calling you!* " hacktivist messages across web forums. Let's find out, in-depth.

The attacks originally starting to take place several weeks before the actual "intervention" with [Georgia President's web site coming under DDoS attack from Russian hackers in July](#) , followed by active discussions across the Russian web on whether or not DDoS attacks and web site defacements should in fact be taking place, which would inevitably come as a handy tool to be used against Russian from Western or Pro-Western journalists. The peak of [DDoS attack and the actual defacements started taking place as of Friday](#) :

"Several Georgian state computer servers have been under external control since shortly before Russia's armed

intervention into the state commenced on Friday, leaving its online presence in dissaray. While the [official website](#) of Mikheil Saakashvili, the Georgian President, has become available again,

the [central government site](#) , as well as the homepages for the [Ministry of Foreign Affairs](#) and [Ministry of Defence](#) , remain down. Some commercial websites have also been hijacked.

The Georgian Government said that the disruption was caused by attacks carried out by Russia as part of the ongoing conflict between the two states over the Georgian province of South Ossetia. In a statement released via a [replacement website](#) built on Google's blog-hosting service, the Georgian Ministry of Foreign Affairs said: "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs."

After defacing Mikheil Saakashvili's web site and integrating a slideshow portraying Saakashvili as Hitler next to coming up with identical images of both Saakashvili and Hitler's public appearances, the site remains under a sustained DDoS attack. It's also interesting to point out that the an average script kiddie wouldn't bother, or wouldn't even understand the PSYOPs effect of coming up with identical gestures of both parties and integrating them within the defaced sites.

What am I trying to imply? It smells like a three letter intelligence agency's propaganda arm has managed to somehow supply the creative for the defacement of Georgia President's official web site, thereby forgetting a simple rule of engagement in such a conflict - risk forwarding the responsibility of the attack to each and every Russian or Russian supporter that ever attacked Georgian sites using publicly obtainable DDoS attack tools in a coordinated fashion.

The DDoS attacks are so sustained that [Georgian President's web site has recently moved to Atlanta](#) :

"The original servers located in the country of Georgia were "flooded and blocked by Russians" over the weekend, Nino Doijashvili, chief executive of Atlanta-based hosting company Tulip Systems Inc., said Monday.

The Georgian-born Doijashvili happened to be on vacation in Georgia when fighting broke out on Friday. She cold-called the government to offer her help and transferred [president.gov.ge](#) and [rustavi2.com](#) , the Web site of a prominent Georgian TV station, to her company's servers Saturday."

[More defacements of news sites and popular Georgian portals](#) started taking place as well :

"Two news websites run by breakaway South Ossetia were hacked on Tuesday morning, officials from the secessionist authorities said. The front page of the website of the news agency, OSinform - **osinform.ru** - which is run by the breakaway region's state radio and television station IR - retained the agency's header and logo, but otherwise the entire page was featuring Alania TV's website content, including its news and images. Alania TV is supported by the Georgian government, and targets audiences in the breakaway region. Another website of the breakaway region's radio and television station - **osradio.ru** - was also hacked. Alania TV has denied any involvement, saying it was itself surprised to see its content on the rival news agency's website."

Ironically, shortly after **Civil.ge** ran the story, it came under DDoS attack, and -- just like Georgia's Ministry of Foreign Affairs -- it switched to a Blogger account in case the site remained unavailable. Moreover, the [Shadowserver posted more details on the command and control servers used in the DDoS attacks](#) , which geolocate back to Turkey and continue to remain online.

"With the recent events in Georgia, we are now seeing new attacks against .ge sites. **www.parliament.ge** & **president.gov.ge** are currently being hit with http floods. In this case, the C&C server involved is at IP address **79.135.167.22** which is located in Turkey. We are also observing this C&C as directing attacks against **www.skandaly.ru** . Traffic from your network to this IP or domain name of **googlecomaolcomyahooocomaboutcom.net** may indicate compromise and participation in these attacks."

As always, this is just the tip of the iceberg, since on **79.135.167.22** we also have several other parked botnet command and control locations, like the following :

emultrix.org yandexshit.com ad.yandexshit.com a-nahui-vse-zaebalo-v-pizdu.com killgay.com ns1.guagaga.net ns2.guagaga.net ohueli.net pizdos.net

Let's analyze the exact way in which the coordinated cyber attack was planned, a weekend's worth of monitoring their activities :

- **distribute a static list of targets, eliminate centralized coordination of the attack**

Who was the only person ever arrested for participating in the Russian vs Estonia cyber "shock and awe" attack? A student who distributed a publicly available list of Estonian government web sites. In the ongoing Russian vs Georgia cyber war, we also have an indication of such lists actively distributed across Russian web forums. And now that the targets to be attacked are publicly known, it's all up to the self-mobilization of the Russian Internet users.

As always, next to the hardcore hacktivists participating in the attack, there are the copycat script kiddies who seem to have found a way to enjoy the media interest into the individuals behind it. Sadly, they have no idea what they're doing, nor how to do it. Here's one such group, **stopgeorgia.ru/stopgeorgia.info** :

"We - the representatives of Russian hako-underground, will not tolerate provocation by the Georgian in all its

manifestations. We want to live in a free world, but exist in a free-aggression and lies Setevom space. We do not need the guidance from the authorities or other persons, and operates in accordance with their beliefs based on patriotism, conscience and belief. You can call us criminals and cyber-terrorists, razvyazyvaya with war and killing people. But we will fight and unacceptable aggression against Russia in Space Network. We demand the cessation of attacks on information and government resources Runeta, as well as appeal to all media and journalists with a request to cover events objectively. Until the situation has changed, we will attack the Georgian government and information resources. Do not we have launched an information war, we are not responsible for its consequences. We call for the assistance of all who care about the lies of Georgian political sites, everyone who is able to inhibit the spread of black information. There is one formal mirror project - www.stopgeorgia.info. All other resources have nothing to do with the movement StopGeorgia.ru.

DRAFT IS UNDER WWW.STOPGEORGIA.RU. IN CASE OF USE
NEDOSTUPNOSTI MIRROR PROJECT -
WWW.STOPGEORGIA.INFO."

- engaging the average internet users, empower them with DoS tools

Following a basic cyber warfare rule , that the masses are sometimes more powerful than the botnet master's willingness to

sacrifice hundreds and thousands of his bots, the current campaign has also thought of the average Internet users who are encouraged to use a plain simple HTTP flooder distributed for this purpose. The concept is nothing new; in fact, this is state of the art cyber warfare combining all the success factors for total outsourcing of the bandwidth capacity and legal responsibility to the average Internet user . Moreover, next to the do-it-yourself tools released, end users who are not so technologically sophisticated are given instructions on how to ping flood Georgian government web sites

- distribute lists of remotely SQL injectable Georgian sites

The last time we witnessed such a tactic aiming to achieve a great deal of efficiency by basically integrating a list of remotely SQL injectable sites into a web site defacement tool, was in May's cyber conflict where Pro-Serbian hacktivists were attacking Albanian web sites by doing exactly the same thing. Surprisingly, Russian hackers have also started distributing lists of Georgian sites vulnerable to remote SQL injections, allowing them to automatically deface them

- abuse public lists of email addresses of Georgian politicians for spamming and targeted attacks

As it appears, a publicly available list of Georgian politics originally created by a lobbying organization, has started to

circulate in an attempt to convince Russian hackers of the potential for abusing it in spamming attacks and targeted attacks presumably serving malware through live exploit URLs

- destroy the adversary's ability to communicate using the usual channels

It's been a while since I've last seen such a pro-active attempt to deny Georgian hackers the ability to communicate through their usual channels. One of Georgia's most popular hacking forums has been down for over 24 hours and continues to be under a permanent DDoS attack on behalf of Russian hackers who have on purposely raised the issue of ensuring that they are unable to reach the local hacktivists and one another. No matter the attack, one should never underestimate other's people's ability to adapt to a certain situation - [The Russian News and Information Agency - RIA Novost, was also a DDoS attack on Sunday](#) :

"RIA Novosti news agency's website was disabled for several hours on Sunday by a series of hacker attacks, as the conflict between Russia and Georgia over breakaway South Ossetia continued for a third day. Websites in both Russia and Georgia have been hit by cyber attacks since Georgia launched a major ground and air offensive to seize control of South Ossetia on Friday. Russia responded by sending in tanks and hundreds of troops. "The DNS-servers and the site itself have been coming under severe attack," said Maxim Kuznetsov, head of the RIA Novosti IT department. RIA Novosti's servers are now functioning as normal."

The aggressiveness of the attacks is prone to accelerate in the next couple of days, due to the combination of the attacks

tactics used, engaging even the less technical hacktivists next to the more sophisticated botnet master. Realizing what's coming, [Estonia has informally offered help to Georgia](#) :

"Estonian officials say that the DDoS attacks targeted against Georgia were very similar to the attacks made against Estonian websites in 2007 after the removal of the Bronze Soldier monument. Unofficially, Estonia and Georgia have been discussing the possibility to send a special team of online security specialists to Georgia. A representative of the Development Centre of State Information Systems said that by now Georgia has not yet made a formal proposal. "This will be decided by the government," said the official."

Who's behind this campaign at the bottom line? As we've already established a connection with well known provider of botnet services

in the previous attack against Georgia President's web site, a connection made possible to establish due to a minor mistake on behalf of the people behind the attack, there's no connection with the current attacks and the Russian Business Network, unless of course you define the Russian Business Network as the script kiddies and the dozen of botnet masters participating who have somehow managed to build their botnets using RBN services in the past, and are now using them against Georgia's Internet infrastructure.

Overall, contingency planning in times when you need to spread a message about what's going in your country, but have

you official government sites logically the de facto information sources in such cases shut down, is crucial for reaching out to the rest of the world who would disseminate the message using the long tail. Then again, this is perhaps the first time in such a cyber conflict --aiming to deny the targeted country's ability to reach the world with real-time information on the real-life warfare events -- [where the targeted country is urging others to obtain this information through a third country President's web site, in this case Poland, and using a blog to do so](#) .

Consumer Reports urges Mac users to dump Safari, cites lack of phishing protection | ZDNet

The 2008 edition of [Consumer Reports' "State of the Net" report](#) , advises that a common security mistake is "thinking

your Mac shields you from all risks", and that due to Safari's lack of built-in phishing protection Mac users are urged to switch to Firefox or Opera :

"According to this year's [State of the Net](#) survey, Mac users fall prey to phishing scams at about the same rate as Windows users, yet far fewer of them protect themselves with an [anti-phishing toolbar](#) . To make matters worse, the browser of choice for most Mac users, Apple's Safari, has no phishing protection. We think it should. What you can do : Until Apple beefs up Safari, use a browser with phishing protection, such as the latest version of Firefox (shown at right) or Opera. Also try a free anti-phishing toolbar such as McAfee Site Advisor or FirePhish."

This is not the first time Apple's Safari has been criticized for lacking built-in phishing protection, and definitely not the last. Earlier this year, [PayPal's Chief Information Security Officer Michael Barrett](#) , said that :

"Apple, unfortunately, is lagging behind what they need to do, to protect their customers. Our recommendation at this point, to our customers, is use Internet Explorer 7 or 8 when it comes out, or Firefox 2 or Firefox 3, or indeed Opera."

For the time being, [Safari is still not considered a "Safe Browser"](#) by PayPal, where safer browser for them means one that

has built-in phishing protection. Whatsoever, the situation always repeats itself. Just like the moment in time when the rest of the now considered "safe browsers" were also lacking phishing protection, third-party plugins were filling in the gaps. The same adaptive approach fully applies to Safari with the help of [1Password's](#)

[integration of the Phishtank.com's database](#) , and also, through the [Soft extension integrating Stopbadware's database](#) next to the rest of the security features it offers.

Related posts:

[Phishers increasingly scamming other phishers](#) [Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails](#) [HSBC sites vulnerable to XSS flaws, could aid phishing attacks](#) [DIY phishing kits introducing new features](#)

Conficker's estimated economic cost? \$9.1 billion | ZDNet

In a recent blog post, the [Cyber Secure Institute](#) claims that based on their previous studies into the average cost of such malware attacks, the economic loss due to the Conficker worm could be as high as \$9.1 billion.

Despite that their analysis also considered a much limited infection rate (200,000 infected hosts), they claim that the cost of the virus in this case is still around \$200 million. The research excludes an important fact though - not only is Conficker still active and infecting, but also, according to the most recent infection rate estimate courtesy of the Conficker Working Group, the [number of infected hosts is 3.5 million](#) .

Here are more details from the analysis:

"Any analysis of the true impact of Conficker must also factor in the (wasted) time, resources, and energies of the cyber-community, governments, companies and individuals. Extrapolating out from studies on the average cost of similar past attacks, the total economic cost of this worm (including the cost of efforts to combat the worm, the cost of purchasing counter-measure software) could be as high as \$9.1 billion. Even using the single, outlying data source that suggests a much more limited scope of infection (<200,000 —vastly less than all other sources suggest—the cost of this virus is still roughly \$200 million dollars."

The number of Conficker infected hosts is in fact much higher than the number provided by the Conficker Working Group in the sense that behind a single IP there may be many other hosts NAT-ed in the local network, adding up yet another variable that has the potential to undermine such estimates. Moreover, the analysis cites that the estimate includes the cost of purchasing counter-measure software, a cost which from my perspective has to be excluded due [to the fact that](#) working [counter-measures](#) are [virtually free](#) due [to the](#) impact of [the worm](#) .

Therefore no additional costs are added for purchasing counter-measure software since based on the current agreements with security vendors, the enterprises are supposed to be automatically protected from the worm.

Go through related Conficker posts: [New worm exploiting MS08-067 flaw spotted in the wild](#) ; [3.5m hosts affected by the Conficker worm globally](#) ; [Conficker worm's copycat Neeris spreading over IM](#) ; [Fake "Conficker Infection Alert" spam campaign circulating](#)

In the past, there have been numerous attempts to estimate the cost of malware, from mi2g's [\\$157 billion and \\$192 billion worldwide loss in 2004](#) due to malware infections, followed by Computer Economics study stating that In 2006, direct damages fell to [\\$13.3 billion, from \\$14.2 billion in 2005, and \\$17.5 billion in 2004](#) . The huge difference of the estimates is due to the different variables taken into consideration by the two companies.

In a perfect world all affected parties would be sharing information on the actual infection rate and the costs due to the worm's infection, thereby confirming that their enterprises have been compromised and potentially ruining business relations for the sake of contributing to the quality of such global studies. In the real world, a Conficker infected international company would try to stay beneath the radar if it can, just as the average Internet user would continue getting exploited through one/two years old client side vulnerabilities, a paradox that's driving cybercrime globally.

Moreover, based on the geolocated chart courtesy of [IBM's ISS](#) and [Symantec's logical conclusion](#) that users, perhaps even companies with illegal copies of Windows represent the largest proportion of the infected set, it's worth pointing out that [denying access to critical patches used as foundation for such worms citing pirated copies](#) , ends up in a situation where the legal owners of the OS would feel the spam/phishing/DDoS/crimeware effect coming from the infected owners of the illegal copies in the long term. Now, would someone located in these countries bother allocating additional resources to protect against Conficker, given that they didn't even bother to purchase the OS at the first place?

Personally, I never take these rough estimates seriously. There are simply way too many variables to take into consideration, especially the worm's global impact, the different allocation for asset protection across the world based on the local economic climate, and the efficiencies and inefficiencies achieved in cleaning malware within a particular company - factors that can greatly decrease or even increase the estimate.

Conficker worm's copycat Neeris spreading over IM | ZDNet

Imitation has always been a form of flattery, and that's particularly true for the cybercrime ecosystem. From the lone [Chinese cybercriminals releasing DIY tools for generating malware](#) actively exploiting the MS08-067 flaw, followed by the original Conficker worm, Microsoft's MMPC (Malware Protection Center) is reporting on a [currently spreading Conficker copycat](#) detected as [Worm:Win32/Neeris.gen!C](#).

The latest variant of Neeris which [has been in the wild since 2005](#), is mimicking all of Conficker's spreading techniques, including the exploitation of MS08-067 and the AutoRun spreading tactic, but is continuing to propagate through its original method - sending links over MSN. With the Neeris copycat now in the game, what are the chances that it would steal some of Conficker's market share? Pretty pessimistic.

The Neeris author also attempted to launch the campaign beneath the radar with Microsoft's MMPC pointing out that the peak of the campaign took place on late March 31st and during April 1st, [Conficker's largely overhyped update activation date](#). However, this tactic is not going to compensate for some of the obvious mistakes that the author made in the form of using bogus time stamps for the malware, and the use of easily spotted as malicious attachments (.exe;.scr) even by the average Internet user.

Copycats don't just share the same propagation/infection vectors, [they also](#) share the same [mitigation ones](#).

Conficker worm to DDoS legitimate sites in March | ZDNet

Among the key innovations of the [Conficker worm \(W32.Downadup\)](#) was the [pseudo-random domain generation algorithm](#) used for the generation of dynamic command and control locations in order to make it nearly impossible for researchers and the industry to take them down. However, once the domain registration algorithm was successfully reverse engineering, it became possible to [measure the estimated number of affected hosts](#) by registering several of the upcoming phone back locations.

What if the Conficker worm suddenly decided that the phone-back locations for March were those of legitimate sites?

[According to Sophos](#) , during March, the millions of Conficker infected hosts will attempt to phone back to several legitimate domains, among which is a Southwest Airlines owned **wnsux.com** , potentially causing a distributed denial of service attack on all of them. Here's a list of the legitimate domains and dates on which Conficker will attempt to contact/potentially DDoS them:

Music Search Engine - **jogli.com** on 8th of March
Southwest Airlines - **wnsux.com** on 13th of March
Women's Net in Qinghai Province - **qhflh.com** on 18th of March
Phonetics by Computer - **praak.org** on 31th of March

In an attempt to mitigate this attack, Southwest Airlines owned **wnsux.com** domains was modified yesterday and is no longer resolving to a particular IP. However, **praak.org** is a redirect to the [University of Amsterdam's Institute of Phonetic Sciences](#) and just like **qhflh.com** and **jogli.com** is still active.

The reverse engineering of the domain registration algorithm not only made it possible to anticipate the upcoming command and control locations, but also, allowed security companies to pre-register them and lock them under the [Conficker Cabal alliance with members such as Microsoft and the ICANN](#) . Moreover, perhaps the most pragmatic mitigation solution implemented on a large scale so

far, has been [OpenDNS updated Stats System which automatically stops resolving Conficker's latest domains](#) , a feature which they introduced last month.

For the time being, the Conficker botnet remains in a "stay tuned" mode with the real malicious payload to be delivered at any particular moment. [A patch has been available](#) since October, 2008.

Conficker graph courtesy of [Microsoft's Malware Protection Center](#)

.

Compromised WordPress sites serving client-side exploits and malware | ZDNet

Security researchers from TrendMicro are reporting on [mass compromise of WordPress sites](#), currently serving client-side exploits and malware to users who click on malicious links in the spamvertised emails connected with the campaign.

According to TrendMicro, cybercriminals are impersonating the Better Business Bureau and LinkedIn in their spamvertised emails, enticing end and corporate users into clicking on the malicious links found in the emails.

Upon clicking on the links, users are exposed to the Black Hole web malware exploitation kits, currently serving CVE-2010-0188 and CVE-2010-1885 exploits, ultimately dropping a [CRIDEX malware variant](#).

Cybercriminals regularly take advantage of compromised legitimate infrastructure acting and distribution and infection vector for their malicious campaigns, in an attempt to trick web filters into correctly identifying the legitimate infrastructure where the distribution and infection vectors are hosted.

End and corporate users are advised to ensure that they're not running [outdated versions of their-party software](#) and [browser plugins](#), as well as to avoid interacting with these emails.

Comparative review: Opera leads in browser anti-phishing protection | ZDNet

According to the most recently released [comparative review by av-comparatives.org](http://comparatives.org) , Opera leads competing browsers in anti-phishing protection. Should you make the switch? Not so fast!

The comparative review used 294 phishing URLs and tested the following browsers:

Apple Safari 5.1.7.7534.57.2

Google Chrome 23.0.1271.97 m

Microsoft Internet Explorer 9.0.9112.16421/9.0.12

Mozilla Firefox 17.0.1

Opera 12.11.1661.

It produced the following results:

Opera: 94.2 percent detection rate of the phishing URLs used in the test

Internet Explorer: 82 percent detection rate for the phishing URLs used in the test

Google Chrome: 72.4 percent detection rate for the phishing URLs used in the test

Apple Safari: 65.6 percent detection rate for the phishing URLs used in the test

Mozilla Firefox: 54,8 percent detection rate for the phishing URLs used in the test.

None of the browsers triggered a "false phishing alarm." What kind of conclusions we can draw based on the these results, and what should decision makers keep in mind when considering a company-wide browser switch?

There's a special crowd of Internet users who are prone to make impulsive switches to a new product or browser, every time a new

study or comparative review is released. That's totally wrong, and here's why:

Time period-specific results: What users and decision makers need to keep in mind is that the results from these comparative reviews are time sensitive, rather than being 100 percent conclusive. And while they offer factual evidence for the performance of a particular product or browser over a specific period of time, the results do not necessarily reflect the big picture, which in 2013 has to do with increased quality assurance (QA) applied by cybercriminals

Built-in phishing protection is among the many other factors to take into consideration before making a switch: Although Opera indeed outperformed competing browsers in anti-phishing protection, it doesn't necessarily mean it outperformed competing browsers when it comes to built-in security mechanisms in general. Case in point: [A Google-commissioned study released in 2011](#) claimed that Chrome is the most secure browser on the market. What the report excluded as a key factor is vulnerable Chrome extensions that could lead to the successful compromise of a host running them. For instance, in 2011, a group of researchers [tested 100 Chrome extensions and found that 27 of them contained 51 vulnerabilities](#). With Chrome leading the global browser wars, it's also worth emphasizing one of the most popular myopias that end and corporate users suffer from nowadays: [the myth of the fully patched Web browser in the context of security](#) .

What some of the browsers tested in the study--but not all of them--have in common is their reliance on the ubiquitous Safe Browsing service, excluding the fact that for years, cybercriminals have been relying on sophisticated "[malicious content cloaking](#) " techniques to prevent Google's crawlers from detecting their fraudulent or malicious content.

Let's discuss the big picture in more detail.

Mono-cultural reliance on Safe Browsing is good for PR, but it doesn't fuel innovation in built-in browser anti-phishing, anti-malware, and anti-client-side exploitation protection; when was the last time your browser of choice announced a new and innovative anti-malware or anti-phishing feature? That's right, it doesn't happen

every day, and not even on a quarterly basis. It is my personal belief that browser vendors have found their "sweet spot" hiding behind the industry-accepted Safe Browsing service, and have therefore failed to innovate on the anti-phishing and anti-malware protection fronts over the past couple of years. The result? Successful detection for low QA malicious campaigns, and zero detection for sophisticated high QA campaigns

The QA applied by cybercriminals has the potential to undermine the real-life applicability of comparative reviews and industry-accepted standards. Ask yourself the following: What would be the first thing you would do if you were to launch a phishing, exploits, and malware serving campaign knowing that millions of users are directly or indirectly protected by Google's Safe Browsing? That's right! You'd not only check whether the service has blocked your URLs, you'd also check those URLs against the most popular Internet security suites on the market. [This Q&A practice](#) has been available to cybercriminals as a service for years, and is currently covering all the major community-based malicious URL-tracking services, next to all the major Internet security suites, leading to a higher probability of successful interaction with the malicious or fraudulent URLs, and millions of users with a "false feeling of security."

Do comparative reviews shape your decision-making process, and in what way? Do you believe that the mono-cultural reliance on the Safe Browsing service is actually protecting more people than helping cybercriminals reach a wider "attack population" thanks to its mass adoption? Do you think browser vendors failed to innovate on the anti-phishing/anti-malware/anti-client-side exploitation fronts over the past couple of years, and what should be done in this direction?

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

CommTouch: 71 percent increase in new zombies | ZDNet

What's the ROI of the ongoing spamvertised notifications ([DHL](#), [USPS](#); [UPS](#), [FedEx](#)) malware campaigns?

According to researchers from CommTouch, since the start of the malware outbreaks, they have recorded a [71% increase in new zombies](#), clearly indicating a pretty decent click-through rate for the malicious attachments.

Meanwhile, [M86 Security is also reporting an increase in malicious spam](#), attributing the growing trend to the ongoing spamvertised notifications and verification order emails. Next to scareware, the researchers also spotted a trojan that aims to seed the [Aprox bot](#) executable in the infected host.

Despite common sense wisdom and numerous warnings [end users continue interacting with links and attachments found in suspicious emails](#).

Commonwealth fined \$100k for not mandating antivirus software | ZDNet

According to a recently published [SEC cease-and-desist order](#) , the Commission has recently fined [Commonwealth Financial Network](#) \$100,000, for not mandating antivirus software on the computers of its representatives, leading to a security incident which took place in November 2008, allowing the cybercriminal behind the attack to place eighteen unauthorized purchase orders, resulting in \$523,000 of unauthorized purchases.

Despite Commonwealth's brisk reaction which greatly minimized the financial impact of the compromised accounts, the incident took place shortly after a representative contacted the IT Help Desk indicating a malware infection might have taken place without receiving "follow-up" attention:

"In or around November 2008, an unauthorized party obtained the login credentials of one of Commonwealth's registered representatives through the use of a malware/keystroke logger virus. The virus was placed on the registered representative's computer, which at the time did not have antivirus software properly employed. The intruder ran a search query for the Commonwealth registered representative's customer accounts with cash balances in excess of a certain amount, generating a list of 368 accounts.

On that same day, the intruder placed or attempted to place eighteen unauthorized purchase orders for the common stock of one publicly-traded company in eight of the 368 customer accounts identified, totaling over \$523,000 of unauthorized purchases. Commonwealth immediately canceled the unauthorized purchases and transferred them into its error account, ultimately absorbing a net loss of approximately \$8,000, and reported the incident to the Commission staff. Commonwealth also notified the owners of the 368 accounts."

With Commonwealth not offering a DIY online trading platform ([Citizens Financial sued for insufficient E-Banking security](#)), which

would have allowed them to forward the responsibility for a potential compromise through a "[No security software, no E-banking fraud claims for you](#) " contract agreement, lacking security E-banking best practices in general, and actual enforcement of them on the computers of their representatives has been exposing their client's financial assets in the most insecure way possible - having them rely on the common sense security practices whose enforcement they took for granted.

Would the presence of antivirus software have made any difference considering the tactics applied by [cybercriminals successfully bypassing signatures-based scanning](#) ? Partly, since it would have at least increased the probability of detection, and mitigated the potential of infection with known malware.

The solution? E-banking on [Live CD or through alternative operating systems](#) in order to bypass a huge percentage of crimeware and the way it currently works, has always been an alternative. However, until financial institutions themselves start building awareness on the concept, and admit that the current E-banking security process is not just flawed, but has been systematically exploited for years, the concept would remain an enemy to the most advantageous of E-banking's features - convenience that millions of users are used to.

Commercial vendor of spyware under legal fire | ZDNet

Just like every decent marketer out there, vendors of commercial malware tools are very good at positioning their tools. However, their pitches often contradict with themselves in a way that what's promoted as a Remote Administration Tool, has in fact built-in antivirus software evading capabilities, rootkit functionality and tutorials on how to remotely infect users over email.

This fake positioning is finally receiving the necessary attention. CyberSpy Software LLC, a [popular vendor of such commercial spyware tools](#) has been recently targeted by the U.S Federal Trade Commission, with the company's sites shut down already. Wish it was that simple.

"Defendants touted RemoteSpy as a "100% undetectable" way to "Spy on Anyone. From Anywhere." According to the FTC complaint, the defendants violated the FTC Act by engaging in the unfair advertising and selling of software that could be: (1) deployed remotely by someone other than the owner or authorized user of a computer; (2) installed without the knowledge and consent of the owner or authorized user; and (3) used to surreptitiously collect and disclose personal information. The FTC complaint also alleges that the defendants unfairly collected and stored the personal information gathered by their spyware on their own servers and disclosed it to their clients. The complaint further alleges that the defendants provided their clients with the means and instrumentalities to unfairly deploy and install keylogger spyware and to deceive consumer victims into downloading the spyware."

Going through a dozen of such tutorials and new releases courtesy of the [illegal vendors](#) of malware daily, the way commercial vendors explain the process of sending the malware is very similar to the way the illegal vendors do it :

"Now it is time to send out the file to the remote PC. In this guide we are using Outlook Express on Windows XP. Click the Create Mail

button to open a new mail window. Click ATTACH and navigate to where you saved your Realtime-Spy file you created previously. Click on the file and then click 'Attach' to attach the file to your email. You will now have to enter a recipient for the file you are sending, as well as an email subject and body. Notice the size of the Realtime-Spy file - it should be approximately 100-115kb at all times! Once you are ready to go click Send to send the email! Note: Users will only appear after they have downloaded and executed the file you have sent them."

Vendors of commercial malware are naturally vertically integrating by not only offering malware for PCs, but also, actively developing mobile malware applications. Both of these are then actively advertised through popular advertising networks, but are mostly driving their traffic from affiliate based programs.

What's the antivirus vendors take on this particular piece of commercial malware? Labeled as [a surveillance tool](#) or [spyware](#) , the majority of them [already detect it](#) . Anyway, [such shut down operations](#) must be done in a "bulk fashion" with a great deal of other commercial malware and keylogging software vendors whose products still remain active online. For instance, the following brands remain active and are operated by other companies whose network of affiliates is reaching a wider audience, with some of the vendors allowing affiliates to re-brand leading to new names for old commercial malware :

"Keystroke Spy, Keylogger Pro, Key Spy Pro, KeyCaptor, Keylog Pro, Invisible Keylogger, SpyAgent, SpyBuddy, Golden Eye, CyberSpy, Screen Spy, AceSpy Spy, SniperSpy, RemoteSpy, Realtime Spy, SpyAnywhere, RemoteSpy, KeySpy Remote, Catch Cheat, Silent Logger, Email Spy Pro; WebMail Spy; Spy Mail; Stealth Email Redirector, Perfect Keylogger for Mac OS X, "

With CyberSpy Software LLC's site now shut down, it would be interesting to monitor whether another company would brandjack the popularity of their products.

Commercial Twitter spamming tool hits the market | ZDNet

Last week, a commercial Twitter spamming tool (**tweettornado.com**) pitching itself as a "fully automated advertising software for Twitter" hit the market, potentially empowering phishers, spammers, malware authors and everyone in between with the ability to generate bogus Twitter accounts and spread their campaigns across the micro-blogging service.

TweetTornado allows users to create unlimited Twitter accounts, add unlimited number of followers, which combined with its ability to automatically update all of bogus accounts through proxy servers with an identical message make it the perfect Twitter spam tool.

TweetTornado's core functionality relies on a simple flaw in Twitter's new user registration process. Tackling it will not render the tool's functionality useless, but will at least ruin the efficiency model. Sadly, **Twitter doesn't require you to have a valid email address when registering a new account**, so even though a nonexistent@email.com is used, the user is still registered and is allowed to use Twitter.

So starting from the basics of requiring a validation by clicking on a link which will only be possible if a valid email is provided could really make an impact in this case, since in its current form the Twitter registration process can be so massively abused that I'm surprised it hasn't happened yet. Once a Twitter spammer has been detected, the associated, and now legitimate email could be banned from further registrations, potentially emptying the inventory of bogus emails, and most importantly making it more time consuming for spammers to abuse Twitter in general.

If TweetTornado is indeed the advertising tool of choice for Twitter marketers, I "wonder" why is the originally blurred by the author Twitter account used in the proof (twitter.com/AarensAbritta) currently suspended, the way the rest of the automatically registered

ones are? Pretty evident TOS violation, since two updates and 427 followers in two hours clearly indicate that a spammer's tweeting.

Commercial spying app for Android devices released | ZDNet

A well known commercial provider of spyware applications for [numerous mobile platforms](#) , has recently ported its [Mobile Spy app to the Android mobile OS](#) .

Just like previous releases of the application, the Android version keeps a detailed log of GPS locations, calls, visited URLs, and incoming/outgoing SMS messages, available at the disposal of the attacker who installed it manually by obtaining physical access to the targeted device.

More details:

"Mobile Spy runs in total stealth mode and no mentions of the program are shown inside the Android device. After the software is set up on the phone, it silently records GPS locations at a rate decided by the owner of the phone. The entire text of all SMS text messages, along with the associated phone number, is also recorded. Additionally, inbound and outbound call information with duration of the call is recorded. Immediately after activities are logged, they are silently uploaded to the user's private online account.

Mobile Spy runs on all Android devices, including the new My Touch 3G by T-Mobile and Motorola Droid. The software also has a version for iPhone, BlackBerry and other smartphones running the Windows Mobile or Symbian OS operating systems. These devices are available from most major mobile carriers."

Despite the company's positioning as a vendor offering the ability to "*silently record SMS text messages, GPS locations and call info of your child or employee* ", two years ago, [F-Secure](#) and Airscanner revealed [trivial security vulnerabilities](#) within the most popular vendors of spyware applications(FlexiSpy and [Retina-X Studios, LLC](#)), allowing anyone easy access to someone else's spying logs.

Others, on the other hand have already [flagged the application as spyware](#) within their [mobile antivirus solutions](#) .

Consider going through related posts: [The future of mobile malware - digitally signed by Symbian?](#) ; [Transmitter.C mobile malware spreading in the wild](#) ; [New Symbian-based mobile worm circulating in the wild](#) ; [New mobile malware silently transfers account credit](#)

Despite the clear commercial interest in releasing such applications, last month [US-CERT warned](#) on the public release of the first free [BlackBerry spying application \(PhoneSnoop\)](#) released by [Sheran Gunasekera](#) at this year's HITBSecConf 2009.

It its current form, Mobile Spy acts and hides like a malware would, however, the day when the vendor starts playing a "cat and mouse" game with antivirus vendors by systematically obfuscating its releases -- like cybercriminals do in order to evade detection -- it would officially join the mobile malware market segment.

Comcast's DNS records hijacked, redirect to hacked page | ZDNet

For a couple of hours yesterday, Comcast's Internet Portal (comcast.net) had its DNS records hijacked and a defaced web

page was loading from third-party domains. Further investigation into this incident reveals a connection between the group responsible for Comcast's DNS hijacking and previous incidents such as the [defacements of Justin Timberlake, Hilary Duff and Tila Tequila's MySpace profiles](#). Comcast.net wasn't hacked, its [DNS records got hijacked](#), so whenever someone visited comcast.net, the defaced page was loading from different servers. Let's assess the incident by taking a look at the way [Comcast's DNS records changed yesterday](#), find out who's behind it, and how a couple of hours later Comcast restored access to its domain.

On 28-May-2008 23:05:43 EDT Comcast.net's WHOIS records were hijacked, and were returning the following information :

Administrative Contact: Domain Registrations, Comcast
kryogenicsdefiant@gmail.com Defiant still raping 2k8 ebk 69 dick
tard lane dildo room PHILADELPHIA, PA 19103 US 4206661870
fax: 6664200187

During that time, the page used in the defacement was loading from two different locations, namely, **freewebs.com /buttpussy69** and **freewebs.com /kryogeniks911** which continue returning the message :

KRYOGENIKS EBK and DEFIANT RoXed COMCAST sHouTz To
VIRUS Warlock elul21 coll1er seven

Due to the changed DNS records, comcast.net was also unreachable for a certain period of time, and within the next couple of hours upon Comcast noticing the incident and taking actions to restore access to their domain, a "Web Site Under Construction" message was appearing.

Comcast's original DNS records returned the their original state on 29-May-2008 01:18:02 EDT :

Administrative Contact: Domain Registrations, Comcast
domregadmin@comcastonline.com Comcast Cable Communications
Mgmt. LLC One Comcast Center 40th Fl. PHILADELPHIA, PA 19103
US 215-286-8665 fax: 6664200187

The hijacking was also picked up by uptime monitoring services, with the longest downtime for the Comcast.net domain for the past three years (98.29%) or 18 minutes :

Tracking down the DNS hijackers using the message left, leads to the well known Kryogeniks group (**kryogeniks.org**) , elul21 (**username.com/tmp**) as another web site defacer part of the WINGS Hacking Team, next to CoLL1er.

Investigation is ongoing, details will posted once more data is gathered.

Comcast responds to passwords leak on Scribd | ZDNet

Comcast has responded to the recently found list of passwords hosted at the popular social publishing site [Scribd](#) . Originally claimed to be [a list consisting of 8000 passwords for Comcast customers](#) , the company now states that not only are 4000 of the passwords duplicates, but also, that only 700 of them belong to active Comcast customers.

Perhaps the result of a phishing campaign that apparently took place a long time ago, this incident highlights several important issues. For instance, the professor at Wilkes University that originally came across the list -- copies of it are still available online -- is disturbed by the fact that he's using this very same leaked password everywhere else - *"That isn't just my password for Comcast, it's my password for everything that is not tied to my credit card, "*. Bad password management practices are clearly in place, but how relevant are these best practices in a situation where the host is already compromised by malicious software? A rhetorical question.

Go through related Comcast security incidents - [Comcast's DNS records hijacked, redirect to hacked page](#) ; [How was Comcast.net hijacked?](#)

In a recently released Gartner document entitled "[Consumers Don't Want to Change the Ways They Manage Online Passwords](#) " the analysts try to raise awareness on the fact that users continue using the same (weak) passwords across different web sites. And whereas the document is reasonably emphasizing on the well known insecure practice, it excludes a simple truth - that a password's strength and diversity of different passwords across web sites, becomes irrelevant practice once a host gets compromised.

Comcast is in a process of notifying the affected customers. Looks like phishing as usual, with an odd choice for hosting the collected data on behalf of the campaigners.

Comcast phishing site contains valid TRUSTe seal | ZDNet

UPDATED with response from TRUSTe. Security researchers from Sophos are reporting on an intercepted [Comcast-themed phishing email, which contains a valid TRUSTe seal](#).

More on the phishing email:

Like many other sites that are compromised to host phishing pages, this one appears to have been compromised through vulnerable FrontPage server extensions. Yes, I said FrontPage. The old Microsoft Office package used for building and publishing web sites. Microsoft discontinued support for FrontPage publishing extensions in 2006 and they have been the source of many web site vulnerabilities over the last 15 years. The fake page is an identical copy of the real Comcast XFINITY login page, and surprisingly includes a fully functional [TRUSTe](#) logo which may lend further credibility to the site.

Cybercriminals often take advantage of [visual social engineering elements](#), by embedding logos of reputable and trusted brands in order to improve of authenticity of their bogus content.

Users are advised to keep in mind the fact that these security and privacy seals often have limited applicability in real-life situations, in particular in the process of ensuring a web site's CIA (Confidentiality, Integrity and Availability).

UPDATED, response from TRUSTe:

TRUSTe is taking appropriate steps to escalate and resolve the situation, as the company takes any attempt to mis-use its brand very seriously. TRUSTe encounters periodic attempts to mis-use its brand. The most common example is a company placing a copy of the TRUSTe Privacy Seal on their website without going through the certification process in some cases the site or page they place the seal on is designed to fraudulently collect customer information. TRUSTe has a well documented procedure to quickly have the seal removed - and when necessary have the site shut down. The

particular instance you raise involved a different scenario whereby an unauthorized party placed a copy of TRUSTe's Privacy Seal onto a webpage and linked the Seal to TRUSTe's Privacy Validation Page.

Upon notification of this issue, TRUSTe initiated its escalation process to have the site shut down. As an added precaution, TRUSTe has identified some security changes which it is implementing to prevent the launch of a Privacy Validation Page linked to the un-authorized use of the Privacy Seal. The company will be rolling this feature out to all of its clients as quickly as possible. TRUSTe will also continue to maintain a separate online directory which enables a user to verify if a specific website they are visiting has been certified by TRUSTe and authorized to display the Privacy Seal plus link to the Privacy Validation Page. I hope this helps provide better insight into the issue and what's being done to resolve it both in the short and long term. Please let me know if you have further questions or are interested in speaking with a TRUSTe representative further.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

CNET's Client-side developer blog serving Adobe Flash exploits | ZDNet

Yesterday, Websense Labs issued an alert regarding a compromised CNET blog, namely the Client-side developer blog

which has been embedded with a malicious javascript code attempting to exploit the visitors through a well known vulnerability in Adobe Flash's player. [Websense's alert](#) :

"Websense Security Labs ThreatSeeker Network has discovered that a CNET Networks site has been compromised. The main page of the CNET Client-side Developer Blog contains malicious JavaScript code that de-obfuscates into an iframe that loads its primary malicious payload from a different host. The malicious code is observed to exploit a known integer overflow vulnerability in Adobe Flash ([CVE-2007-0071](#)). At the time of this alert, the site is still hosting the malicious code. Visitors who are not patched against this vulnerability will be infected without any user interaction."

Interestingly, the second javascript obfuscation that they analyzed in the time of detection is different than the one I managed to obtain from a copy of the blog on the 2nd of August. And while it remains unknown for how long has the blog been embedded with the javascript with the, this malware attack, and the rotating javascripts indicate a compromise compared to the massive SQL injections we're seeing on daily basis. The embedded javascript code appears to have been removed. Deobfuscating the obfuscated javascript code, attempts to access the live exploit URL from a .info domain that is now down. Historically, the same domain has been used in blackhat search engine optimization campaigns - yet another example of underground multitasking, namely, abusing a single domain for several different fraudulent purposes.

This malware attack should not be treated as an isolated event, it's the result of today's major risk-forwarding process, where legitimate sites are starting to serve malware and exploits with an unprecedented growth. Multiple vendors are confirming the trends,

for instance, in its latest report, [ScanSafe reports 407 percent increase in compromise of legitimate websites](#) , followed by Sophos, [according to which a full 79% of malware-hosting Web sites are legitimate ones](#) , and with Websense stating that [more than 75 percent of the Web sites it classified as malicious were actually legitimate ones](#) .

Slowly, but inevitably, the "*do no visit unknown and potentially harmful sites* " security tip is starting to lose its charm.

Click fraud in 2nd quarter of 2008 more sophisticated, botnets to blame | ZDNet

Whereas the overall click fraud rate isn't increasing, it's not decreasing either, remaining flat for the first two quarters of

2008, according to data gathered from the Click Fraud Network, consisting of more than 4,000 online advertisers and agencies. Click Forensics report for the second quarter of 2008, indicates that botnets continue being used for click fraud, the preferred and more efficient approach compared to hiring human clickers on a revenue sharing basis. [Here are some of the key findings from data reported for Q2 2008](#) :

The overall industry average click fraud rate was 16.2 percent for Q2 2008. That's down slightly from the 16.3 percent rate reported for Q1 2008 and up from the 15.8 percent click fraud rate reported for Q2 2007

The average click fraud rate of PPC advertisements appearing on search engine content networks, including Google AdSense and the Yahoo Publisher Network, was 27.6 percent. That's down from the 27.8 percent rate reported for Q1 2008 and up from the 25.6 percent average click fraud rate reported for Q1 2007

For the first time, traffic from botnets was responsible for more than 25 percent of all click fraud traffic in Q2 2008

In Q2 2008, the greatest percentage of click fraud originating from countries outside North America came from China (4.3 percent), Russia (3.5 percent), and France (3.2 percent)

In previous Zero Day coverage for Q1 2008 ([Botnets committing click fraud observed](#)), we've already discussed the most common click fraud scheme in general, consisting of underground traffic exchange networks and renting botnet services, using an sampled activity from a single such affiliate based network showcasing that :

"1,264,204 bots that did 3,095,194 searches and 537,764 clicks made a total revenue of \$5, 495, which when deducting percentage for the affiliate coordinating the campaigns, ends up with a profit of

\$3,605 - this is a great example of greedy affiliate managers taking high commissions."

Let's discuss the dominating click fraud scheme in Q2, consisting of an ugly combination of botnet ownership and a huge portfolio of parked domains serving ads which deliver revenue to the person behind the scheme.

Click fraud in Q2 2008 is said to be getting more sophisticated due to several new developments that greatly contribute to increasing activity on multiple cybercrime fronts. The fact that the greatest percentage of click fraud clicks is coming from China, is the direct result of [a growing infrastructure that cannot be properly secured](#) , and with over [4 million new ADSL subscribers in China for the first half of the year](#) , these very same folks shape the threatscape by suffering their first malware infection, whose first-timer always-on Internet experience is a juicy target for even the most obvious types of malware attacks.

The second, and perhaps most important key development leading to the increasing sophistication of click fraud done through botnets, is that the people behind these scams are starting to put more efforts into ensuring that the junk content created at their web sites would increase the probability of having their botnet click on highly popular and consequently very expensive keywords, thereby earning more on a per click basis. Coming up with an approximate price for a keyword is done through [third-party services keeping track of popular keywords](#) . In fact, sometimes keywords in the content are irrelevant if they start taking advantage of typosquatted domains so descriptive that they'll attract a great deal of relevant and high priced ad links on hundreds of thousands of parked domains.

The abuse of parked domains is among the main reasons why [Google is facing another click fraud lawsuit](#) :

"In the new lawsuit, online retailer RK West, which operates the online store Malibu Wholesale, alleges it purchased ads Google without realizing they would appear on parked domains. Parked domains typically have no content other than ads. RK West alleges that many of the clicks generated by parked domains are "invalid."

The company said in its lawsuit that it had been charged for clicks from parked domains "that had little relation to its business."

"Despite indication that some of the clicks from parked domains were invalid, Google failed to disclose to the plaintiff specific domain names in which these ads were clicked on, making detection of invalid clicks difficult and even worse concealing any evidence of invalid clicks," the lawsuit alleges. RK West eventually went through its server logs and discovered the source of the clicks, said Alfredo Torrijos, one of the company's attorneys. "

Botnets are doing what they've always been doing, committing click fraud on behalf of those who've researched and exploited news schemes and tactics. The problem can be at least partly minimized by ensuring that known malware infected hosts who've been spamming, phishing, and generally those who are not to be trusted, and any of their interactions not just on the authentication level in order to prevent them from registering a couple of hundred bogus email addresses, are either challenged, or their clicks flagged as highly suspicious.

Click fraud facilitating Bahama botnet steals ad revenue from Google | ZDNet

Originally exposed as a botnet redirecting and monetizing [hijacked traffic to over 200,000 parked domains](#) primarily located in the Bahamas, [researchers from ClickForensics](#) have recently found evidence on active DNS hijacking of Google properties allowing cybercriminals to steal revenue from Google by pulling search results and displaying them on a bogus homepage ([Cybercriminals promoting malware-friendly search engines](#)) which serves ads from pay-per-click ad networks ([Microsoft's Bing invaded by pharmaceutical scammers](#)) maintained by similar cybercrime enterprises.

Here's how Bahama's click fraud scheme steals ad revenue from Google and its advertisers according to ClickForensics:

However, in the case of the Bahama Botnet, this DNS translation method gets corrupted. The Bahama botnet malware causes the infected computer to mistranslate a domain name. Instead of translating "Google.com" as **74.125.155.99** , an infected computer will translate it as **64.86.17.56** . That number doesn't represent any computer owned by Google. Instead, it represents a computer located in Canada.

When a user with an infected machine performs a search on what they think is google.com, the query actually goes to the Canadian computer, which pulls real search results directly from Google, fiddles with them a bit, and displays them to the searcher. Now the searcher is looking at a page that looks exactly like the Google search results page, but it's not. A click on the apparently "organic" results will redirect as a paid click through several ad networks or parked domains -- some complicit, some not. Regardless, cost per click (CPC) fees are generated, advertisers pay, and click fraud has occurred.

The click-fraud scheme ([Botnets committing click fraud observed](#)) affects all of Google's international domains, with the actual DNS

records hijacking taking place upon infection with scareware ([The ultimate guide to scareware protection](#)) pushed by the gang's portfolio of compromised domains serving bogus [content syndicated from Google Trends](#) in real-time.

The cybercrime enterprise behind the Bahama botnet is also linked to the recent [malvertising_\(malicious ads\) incident that affected the web site of the New York Times](#) , the [Koobface botnet](#) , as well as to a huge percentage of the [blackhat search engine optimization](#) campaigns [serving scareware](#) analyzed throughout the past couple of months.

Citizens Financial sued for insufficient E-Banking security | ZDNet

If a fraudulent transaction ever takes place on one of your bank accounts due to their compromise, who's to blame - the bank, for not providing you as a customer with state-of-the-art security mechanisms that could have prevented it, or you, as a customer whose insecure online behavior led to the compromise at the first place?

In the [Shames-Yeakels vs Citizens Financial lawsuit](#), a couple that lost \$26,500 due to a compromised account, may have all the good reasons to blame their bank's outdated E-banking authentication process, which in 2009 is a combination of SSL connection next to a user name and a password, with no sign of two-factor authentication in place:

At the time of the theft, Citizens had been in the process of issuing such tokens to customers, but the plaintiffs say they were too slow in rolling out this security measure. They pointed to a 2005 document from the Federal Financial Institutions Examination Council, which concluded that single-factor authentication was inadequate, and said that Citizens lagged behind other banks in offering this feature.

Citizens used a company named Fiserv to provide its online banking services, including information security services, and argued that Fiserv had a solid reputation in the banking industry and that its security measures were not the cause of the money transfer.

Would two-factor authentication have made any difference at the first place? That largely depends on the banker malware/crimeware that the customer gets infected with, since three of the most popular crimeware applications that used to be proprietary tools in the arsenal of the sophisticated cybercriminal a couple of years ago, are not just publicly available nowadays, but are all capable of bypassing badly implemented two-factor authentication solutions in place.

The success of these crimeware applications is so evident, that the number of [managed crimeware services](#) offering access to

[banker malware infected hosts](#) , or raw logs of their E-banking authentication process for the purpose of session hijacking, is increasing and is therefore lowering the entry barriers into a market segment that used to be reserved for the more technically sophisticated cybecriminals a couple of years ago.

Go through related posts: [75% of online banking sites found vulnerable to security design flaws](#) ; [HSBC sites vulnerable to XSS flaws, could aid phishing attacks](#) ; [CardCops: Stolen credit card details getting cheaper](#) ; [Scammers caught backdooring chip and PIN terminals](#) ; [Scammers introduce ATM skimmers with built-in SMS notification](#) ; [Diebold ATMs infected with credit card skimming malware](#) ; [Antivirus vendor introducing virtual keyboard for secure Ebanking](#) ; [No security software, no E-banking fraud claims for you](#)

SSL connections combined with "secure user name" and a password can't protect against sophisticated cybercriminals, in fact they can't even protect you from the average ones still relying on outdated approaches of obtaining accounting data through the use of keyloggers. What two-factor authentication and a decent understanding of the current/emerging threats can do, is mitigate a significant percentage of the risk that would have otherwise resulted in a successful compromise with less efforts on behalf of the cybercriminal.

What do you think? Who's to blame for the fraudulent transaction in this case - the couple which apparently was E-banking from a crimeware infected computer, or the bank for not offering two-factor authentication at the first place?

Talkback.

Chrome 20 fixes 20 security vulnerabilities | ZDNet

In its latest browser release, 20.0.1132.43, [Google's Chrome fixes 20 security vulnerabilities](#), none of which are critical.

More details on the vulnerabilities:

- [CVE-2012-2815](#) : Leak of iframe fragment id
- [CVE-2012-2816](#) : Prevent sandboxed processes interfering with each other
- [CVE-2012-2817](#) : Use-after-free in table section handling
- [CVE-2012-2818](#) : Use-after-free in counter layout
- [CVE-2012-2819](#) : Crash in texture handling
- [CVE-2012-2820](#) : Out-of-bounds read in SVG filter handling
- [CVE-2012-2821](#) : Autofill display problem
- [CVE-2012-2822](#) : Misc. lower severity OOB read issues in PDF
- [CVE-2012-2823](#) : Use-after-free in SVG resource handling
- [CVE-2012-2824](#) : Use-after-free in SVG painting
- [CVE-2012-2826](#) : Out-of-bounds read in texture conversion
- [CVE-2012-2827](#) : Use-after-free in Mac UI
- [CVE-2012-2828](#) : Integer overflows in PDF
- [CVE-2012-2829](#) : Use-after-free in first-letter handling
- [CVE-2012-2830](#) : Wild pointer in array value setting
- [CVE-2012-2764](#) : Unqualified load of metro DLL
- [CVE-2012-2831](#) : Use-after-free in SVG reference handling
- [CVE-2012-2832](#) : Uninitialized pointer in PDF image codec
- [CVE-2012-2833](#) : Buffer overflow in PDF JS API
- [CVE-2012-2834](#) : Integer overflow in Matroska container

Users are advised to restart their browsers in order to update to the latest version of Chrome. They can also do so manually, by selecting the "About Google Chrome" option in the settings menu.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Chinese hackers launch targeted attacks against foreign correspondents | ZDNet

According to an assessment published by [the Information Warfare Monitor](#) , Chinese hacktivists (politically motivated hackers) have recently launched a targeted malware attack against foreign news correspondents attempting to trick them into executing a malware-embedded PDF attachment ([Interview list.pdf](#)), coming from [a non-existent editor working for The Straits Times](#) .

The attacks coincide with the upcoming nation-wide celebration of the [60th anniversary of the PRC](#) , and appear to be directly connected to the [GhostNet cyber espionage network](#) exposed earlier this year.

Key findings of the assessment include:

The content of the email, and the accompanying malicious attachment, are in well written English and contain accurate information. The email details a reporter's proposed trip to China to write a story on China's place in the global economy; all the contacts in the malicious attachment are real people that are knowledgeable about or have a professional interest in China's economy.

The domain names used as "command & control" servers for the malware have been used in previous targeted attacks dating back to 2007. The malware domain names, as in previously documented cases, only resolve to real IP addresses for short periods of time. The malware exploits vulnerabilities in the Adobe PDF Reader, and its behaviour matches that of malware used in previous attacks dating back to 2008. This malware was found on computers at the Offices of Tibet in London, and has used political themes in malware attachments in the past.

The IP addresses currently used by the malware are assigned to Taiwan. One of the servers is located at the National Central University of Taiwan, and is a server to which students and faculty connect to download anti-virus software. The second is an IP address assigned to the Taiwan Academic Network. These

compromised servers present a severe security problem as the attackers may have substituted their malware for anti-virus software used by students, employees, and faculty at the National Central University.

The most logical approach to obtain the emails of the targeted correspondents in order to facilitate this social engineering based malware attack, would be to compile a list based on publicly obtainable data. The same practice was in planning stage but never got executed during the [coordinated Russia vs Georgia cyber attack](#) , when emails corresponding to government agencies were "harvested" for [potential targeted malware attacks](#) .

Go through related posts: [Chinese hackers deface the Russian Consulate in Shanghai](#) ; [China detains web site defacer spreading earthquake rumors](#) ; [China busts hacking ring, managed to penetrate 10 gov't databases](#) ; [Chinese female hacking group spotted](#) ; [Chinese Hacktivists Waging People's Information Warfare Against CNN](#) ; [The DDoS Attack Against CNN.com](#)

However, the researchers behind [the assessment](#) make an interesting observation. According to a Reuters article stating that the names of the targeted correspondents do not appear on public news reports and that they were hired through an agency that reports to [China's Foreign Ministry](#) , they raise an element of suspicion regarding the ways in which the attackers obtained emails that were supposedly not available to the public. In reality, though, this appears to be a simple data mining process relying on either already compromised hosts of foreign or Chinese journalists, or on the use of public search engines allowing the malicious attackers to easily build their "hit lists".

Whether a trend or an isolated incident coinciding with the 60th anniversary of the PRC, [China's cyber espionage ambitions](#) remain as high as ever.

Chinese hackers deface the Russian Consulate in Shanghai | ZDNet

That was fast. [Chinese hackers](#) collaborating with the Chinese Hacking Union, a two-years old training community for wannabe hackers, hacked and defaced the official web site of [the General Consulate of the Russian Federation in Shanghai, PRC](#) in response to the recent accusations that a [Russian navy vessel has sank a Chinese cargo ship](#) .

The message left on the now "under maintenance" site translates as follows:

"Russia invaded our territory to kill people from the People's Republic. Hack done for the Chinese crew of controversy! Russia must be punished! !! Hacked BY: Yu"

In a related interview, profiling the hacker "Yu" after the Russian Consulate hack, he describes himself as a network security enthusiast that has been defacing Chinese, Japanese, Korean, Taiwanese and U.S sites for a while, but had to give up his activities due to college studies. Interestingly, he's also insisting that education is the better choice in the long term, than the web site defacements he's involved into.

Go through related hacktivism/political hacking incidents - [Pro-Serbian hacktivists attacking Albanian web sites](#) ; [Hundreds of Dutch web sites hacked by Islamic hackers](#) ; [300 Lithuanian sites hacked by Russian hackers](#) ; [Georgia President's web site under DDoS attack from Russian hackers](#) ; [Coordinated Russia vs Georgia cyber attack in progress](#) ; [Thousands of Israeli web sites under attack](#)

Yu's hacking group, as well as the Chinese Hacking Union, are a great example of the diverse but highly [de-centralized province-based IT underground scene in China](#) . Largely inspired by the glorious **China Eagle Union** , the **Red Hacker's Alliance** and the **Hacker Union of China** , new training communities keep popping-up like mushrooms - even gender based ones ([Chinese female hacking group spotted](#)).

The site of the Russian Consulate in Shangha remains serving a
*"The site is currently under maintenance! sorry for any
inconveniences!"* message.

Chinese female hacking group spotted | ZDNet

Chinese girls talking about using SQL injections to serve malware and ARP spoofing, in between sharing do-it-yourself tutorials on XSS worms? Sexy. Scott Henderson at the Dark Visitor profiled a Chinese [hacking_group_with_female_members](#) only, discussing these very same topics :

"In the male dominated world of Chinese hackers, females find it difficult to be accepted as equals. Their technical skills are often viewed as inferior to their male counterparts. As far as I am aware, the first group of female Chinese hackers to break this mold were the Six Golden Flowers. The Golden Flowers have since broken up and gone their separate ways, but a new and larger group has taken their place, the Cn (China) Girl Security Team. The website for the China Girl Security Team was registered on 12 Mar 2007 and currently has 2,217 members. The leader of the group Xiao Tian, is only 19 years old"

What you should make distinction between are [the hardcore Chinese hacktivists](#) whose understanding of how to wage [people's information warfare](#) was most recently demonstrated in [the Ani-CNN campaign](#) where they've managed to recruit hundreds of thousands of [wannabe hacktivists for participating in the attacks](#) , and [the average script kiddies](#) like these ladies localizing to Chinese well known security papers and actively promoting the download and use of hacking tools. Excluding the perspective that these very same "average script kiddies" turn into quite a threat when empowered, motivated, and coordinated, what are the chances we could witness a "cyberwar of the sexes" in the Chinese underground?

China's 'secure' OS Kylin - a threat to U.S offensive cyber capabilities? | ZDNet

Picture a cyber warfare arms race where the participating countries have spent years of building offensive cyber warfare capabilities by exploiting the monoculture on one another's IT infrastructure.

Suddenly, one of the countries starts migrating to a hardened operating system of its own, and by integrating it on systems managing the critical infrastructure it successfully undermines the offensive cyber warfare capabilities developed by adversaries designed to be used primarily against Linux, UNIX and Windows.

That's exactly [what China is doing](#) right now with their [hardened OS Kylin](#) according to Kevin G. Coleman, Senior Fellow and Strategic Management Consultant with the [Technolytics Institute](#) who presented his viewpoint in a hearing at the [U.S. – China Economic and Security Review Commission](#) .

Here's an excerpt from the hearing:

"Chinese authors believe the United States already is carrying out offensive cyber espionage and exploitation against China. China therefore must protect its own assets first in order to preserve the capability to go on the offensive. While this is a highly unpopular statement, WE ARE IN THE EARLY STAGES OF A CYBER ARMS RACE AND NEED TO RESPOND ACCORDINGLY!

This race was intensified when China created Kylin, their own hardened server operating system and began to convert their systems back in 2007. This action also made our offensive cyber capabilities ineffective against them given the cyber weapons were designed to be used against Linux, UNIX and Windows."

Kylin is an operating system developed by the the University of Science and Technology for National Defense, and successfully approved by China's 863 Hi-tech Research and Development Program office in 2006. According to their web site, the OS has already achieved one of the highest national data security standards,

and is therefore to be used as critical military and government servers. Is Kylin so [unique and impenetrable as China is pitching it](#) , following years of research and piles of money spent on branding it as the secure national operating system of choice? [That may not be the case](#) .

In a [recently conducted kernel similarity analysis](#) , a Chinese student debunks this notion by pointing out that not only are different versions of Kylin's kernel virtually the same, but also, that most of the kernel code is identical to the one of FreeBSD5.3:

"A Linux specialist who declined to be named, said recently that of all the Linux kernel codes, none are developed by Chinese. The situation has been acknowledged by Ni Guangnan, an academic with the Chinese Academy of Engineering and a strong advocate of Linux in China.

Prior to this, the Kylin operating system - which is funded by the National 863 High-Tech Program - was found to have plagiarized from the FreeBSD5.3. An anonymous internet user, who goes by the handle name "Dancefire", pointed out similarities between the two systems reached 99.45 percent."

All warfare is indeed based on deception, especially when you're re-branding.

The rush to participate in the "national security operating system" arms race is pretty evident across the world, with the [European Union's](#) secure [OS Minix](#) , the [U.S Air Force](#) new '[secure distribution of Windows XP](#) ' and Russia's interest in a [similar secure OS](#) .

What everyone appears to be forgetting is the fact that security is proportional with usability, and as well as the fact that [complexity is the worst enemy of security](#) . Combined, these complexities and usability issues end up in not so surprising results such as the [recently conducted pen testing audit at the U.S Federal Aviation Administration](#) , where the auditors from KPMG logically bypassed the "security through secure OS mentality" and by [attacking the upper layers of the OSI Model](#) presented the following results:

"We tested 70 Web applications, some of which are used to disseminate information to the public over the Internet, such as

communications frequencies for pilots and controllers; others are used internally within FAA to support eight ATC systems. Our test identified a total of 763 high-risk, 504 medium-risk, and 2,590 low-risk vulnerabilities, such as weak passwords and unprotected critical file folders."

Upon exploitation of the Web applications, they were able to gain unauthorized access to a Traffic Flow Management Infrastructure system, Juneau Aviation Weather System, and the Albuquerque Air Traffic Control Tower, an ATC system used to monitor critical power supply at six en route centers, and had the capability to install malicious code on users' computers part of FAA's network. How did they do that? By exploiting the basic insecurities that every 'secure' OS has, in this case exploiting the insecurely configured web applications allowing them to gain access, next to exploiting the unpatched ones or the usability and complexity altogether.

The bottom line - are secure operating systems the cornerstone for a hardened critical infrastructure, or is a misconfigured 'secure' operating system just as insecure as the supposedly insecure one in general, managing assets through a flawed and outdated risk assessment process? Talkback.

China's Blue Army: When nations harness hacktivists for information warfare | ZDNet

China has recently announced the existence of [the Blue Army](#), a government sponsored cyber warfare unit similar to those launched by the [U.S](#), the [United Kingdom](#), [Australia](#) and [Israel](#) .

Although the majority of the cyber warfare units have been established for defensive purposes, it's the offensive cyber capabilities that are worth discussing in the context of establishing a borderline for offensive cyber operations. The methodology used in offensive cyber warfare operations is fairly simple - [if you're attacking us we reserve ourselves the rights to strike back at you.](#)

It's a methodology that is totally wrong, taking into consideration the fact that the attack may be coming from a country that is basically abusing the infrastructure of another country, in a combination with reliance of localized attack kits and tactics typical to those used by what is originally perceived as the attacking country.

It's been a decade since the release of the Chinese "[Unconventional warfare](#) " book, and a lot has changed from a conceptual perspective. From symmetric to asymmetric shift in the concepts, to the currently in progress of implementation unrestricted warfare military doctrines, the Chinese has proven that they they're not just able to keep up with the developing environment, but to dominate it with new concepts in cyberspace.

See also: [Should a targeted country strike back at the cyber attackers?](#)

What constitutes unrestricted warfare in the cyberspace realm, really? Basically, it's the reliance on civilians for executing government sponsored or government tolerated cyber operations, the so called [people's information warfare concept](#) . The concept is fairly simple. Instead of establishing a dedicated cyber warfare unit, a country such as China is actively harnessing the potential of

its hacktivist community for executing military operations and activities across the Web.

A number of questions remain for each and every cyber warfare department compared to the [people's information warfare](#) empowered civilians:

Would they be allowed to embed sites of human rights watch activists with malicious software, and develop custom malware?

Would they be allowed to hijack an existing botnet for the purpose of [data mining for OSINT-gathering practices?](#) Would they be allowed to launch offensive cyber warfare practices such as Denial of Service attacks against compromised infrastructure residing in a 3rd country?

Would take take into consideration [island hopping tactics](#) before striking back?

Would they be allowed to develop practical web exploitation tools assisting in massive exploitation attacks?

To what degree would they be allowed to outsource their operations to providers of malicious underground services, instead of developing in-house solutions?

The answer to the majority of these is probably no, as the majority of these tasks are already actively executed by the [Chinese cybercrime underground](#) and the extremely vibrant hacktivist community inside the country -- *China Eagle Union* , the *Hacker Union of China* , and the *Red Hacker's Alliance* for starters. This has become possible due to the China's military realization of the untapped potential for asymmetric cyber dominance, thanks to the government tolerated and nurtured vibrant hacktivist community.

See also: [Attack of the Opt-In Botnets](#)

The Chinese underground and hacktivist community is developed well enough to manage the tasks of a fully operational cyber warfare unit, because it relies on the people not on the department.

The net is vast and infinite, and trying to establish a borderline for cyber warfare operations based on the actions of the actual cyber warfare units, and not on the vibrant hacktivist communities and cybercrime underground within the countries, is totally wrong.

China detains web site defacer spreading earthquake rumors | ZDNet

The Xinhua [news agency is reporting](#) that the web site defacer which I mentioned [in a previous post](#) regarding the use of

web site defacements as tools for psychological operations, has been located and detained in less than a week after he defaced the Seismic Emergency and Public Center of the Guangxi province where he left a fake message on an upcoming earthquake that's going to hit China.

[Tracking him down](#) and [releasing detention clips to the Chinese media](#) is one of these emblematic cyber crime cases the Chinese Cyber Police would do anything to solve. Would they also be allocating the same resources to another incident if it wasn't the momentum and the boldness of this hacker to do what he did in times when China's shaken by earthquakes?

Xinhua has more details :

"Chen, 19, worked in a technology company after graduating from junior middle school. He said he hacked the site to show off his computer skills and have "fun," according to the police.

The administration website was found to have been hacked on May 31. A notice mourning the victims of the 8.0-magnitude quake had been revised to read: "Please prepare for an earthquake with a magnitude of more than 9.0 in Guangxi," Tang said

The news scroll, meanwhile, had been replaced with a single phrase: "Experts warn of earthquake in Guangxi in the near future," he said. "

There are three types of web site defacers, the average ones basically greeting their team members without deleting anything, the commercial ones, that would [monetize their defacement](#) by selling the access to the web server to spammers and malware authors, and the stupid ones, who would deface the Seismic Emergency and

Public Center of the Guangxi province in times when China's shaken by earthquakes and leave a note on yet another one coming.

What is this case demonstrating us anyway? That when there's a will, there's always a way. Most importantly, that when you cannot stop being [the number one hosting_provider_of malware](#) , and malware command and control interfaces in the world, you pick up a single bee out of the beehive and slap it with a newspaper in front of everyone.

China confirms security flaws in Green Dam, rushes to release a patch | ZDNet

China's Ministry of Industry and Information Technology has [instructed the developers of the Green Dam censorware](#) , to briefly release a patch in regard to last week's published analysis detailing the possibility of [remotely exploitable vulnerabilities within the software](#) .

Jinhui Computer System Engineering Co, developer of [Green Dam](#) , insisted that the software is just as vulnerable as any other, and that their expertise is in coding Internet filtering software, and not necessarily one with security in mind -- pretty interesting comment taking into consideration the fact that the [developer earned millions in the process of coding it](#) .

Moreover, despite the fact that Green Dam made the headlines in 2009, and quickly received the necessary reverse-engineering attention which exposed the security flaws within, the vulnerable version of censorware has been shipped to Chinese users as of early 2008.

According to [Green Dam's web site](#) , as of April, 2009 there have been over 3.5 million downloads of the software. In less than a month, following an advertising campaign that featured download link at 160 of China's most popular web sites, the [number of downloads peaked at 7,172,500](#) with the majority of [Chinese provinces, schools and universities](#) having already installed it on their networks.

This massive adoption can in fact quickly mature into the security disaster, researchers Scott Wolchok, Randy Yao, and J. Alex Halderman talked about in their analysis, and exploitation of the software may have already been taking place without any public reports of it.

With China's recent announcement that it [make the censorware an inseparable](#) part of each and every Windows running PC purchased after the 1st of July, through [an agreement with China's Lenovo](#) , it

may well be contributing to the creation of the "Great Botnet" of China.

The vendor of Green Dam is also planning a legal action against the reverse engineering of its product according to a quote published in People's Daily Online. [Zhang Chenmin](#) , manager at Zhengzhou-based Jinhui Computer System Engineering Co. :

"expressed anger at Halderman's report. "It is not responsible to crack somebody's software and publish the details, which are commercial secrets, on the Internet. They (the professors) have infringed the copyright of our product. "I think the negative comments and attacks on Green Dam are intentional," Zhang said, adding his company plans to take legal action against the professors."

I wonder whether they'd still be having the same attitude if malicious attackers used Green Dam's trivial remotely exploitable vulnerabilities, for creating a botnet whose size would have made [Conficker](#) look like an operation run by amateurs.

China busts hacking ring, managed to penetrate 10 gov't databases | ZDNet

If you needed a university certificate in China during the last couple of months, there's a big chance that a group of ten

people could have supplied with you such, going a step further and adding your details in more than ten government databases across different provinces in the country, making \$300k in the process.

[Shanghai Daily is reporting on this sophisticated group of local hackers](#) who were selling "valid" educational certificates by modifying government databases. How they got caught? Apparently, by cross-checking the validity of the certificate, and since they couldn't hack each and every database in order to add a reference to it, their business model was quickly detected and shut down.

"The suspects sold fake certificates to make money. Since authentic certificates can be checked on government Websites, they allegedly attacked databases and added false information, the report said. The scheme was discovered after someone purchased a fake doctor's certificate to apply for a business license in Zhejiang Province in June. Zhejiang authorities found the certificate was faked even though the information on the Jiangxi Public Health Department's Website matched it, the report said. The Jiangxi Public Health Department checked the database and found it was attacked several months and that many statistics were distorted. It reported the case to police."

Whereas [China has a very strong reputation on dealing with local cybercrime attacks in a very short time frame](#), it has perhaps one of the worst reputations across the globe when it comes to the big picture, with Chinese networks topping each and every chart on malicious Internet activity. Is there a double standard on fighting cybercrime in China? Depends. There's no shortage of organizational bodies fighting cybercrime in the country, however, as in many other countries there seems to be a lack of political

awareness on how severe the situation has gotten while they were trying to assess its severity, a situation which when combined with the lack of right priorities set, speaks for itself.

As far as this hacking ring is concerned, once the people behind it could add authentic entries into the database, they could have also taken a peek at others, which in the context of China's overall bureaucratic mentality for anything related to cybercrime, could easily turn into a major espionage case -- or they can easily make it look like one. Moreover, when there's demand for a particular good or a service, there's also supply :

"Li said demand for fake certificates was strong, according to the report. He contacted his friend surnamed Wang to attack the government databases and validate his false certificates, the report said. The investigation showed Wang attacked more than 10 government databases in Jiangxi, Hubei, Guizhou, Sichuan, Jiangsu and Liaoning provinces from March this year. Wang sold the user rights of every database to Li for 5,000 yuan to 8,000 yuan, the report said."

From a security perspective, detecting the fake certificate seems to have worked since these provinces are either not syndicating their databases and trusting a single database as a central point which when once hacked and modified could distribute false data across the rest of the provinces, or the data was cross-checked via offline sources or historical copies of the database. If bureaucracy can help fighting cybercrime by ensuring that a clerk doesn't trust everything he sees on his monitor, and prompts him to cross-check with different databases "just for the record", then that's one of those rare cases.

'Checkout Your PROFILE Stalkers' scam spreading on Facebook | ZDNet

Multiple users are reporting on a currently circulating "Checkout Your PROFILE Stalkers" Facebook scam. Spamvertised as:

OMG! Its unbelievable now you can get to know who views your facebook profile.. i can see my top profile visitors and i am so shocked that my EX is still creeping my profile every hour

Upon clicking on the link, the users are exposed to a "copy and paste propagation technique" where they are asked to copy and paste obfuscated Javascript into their browsers, leading to the re-posting of the same message on their friends' walls.

Users are advised not to interact with the script and report the site as malicious one.

See also:

[Osama execution video scam spreading on Facebook 'Enable Dislike Button' scam spreading on Facebook](#)

CardCops: Stolen credit card details getting cheaper | ZDNet

The dynamics of the underground marketplace are pretty similar to that of the legitimate marketplace, with cybercriminals demanding and supplying, consolidating and start to work together, and coming up with new monetization approaches in order to continue enjoying the high profit margins of their goods and services. The once highly exclusive market segment of stolen credit card details, is today's commodity market segment trading with a virtual asset that has become so prevalent, that cybercriminals are already bargaining with it.

Taking into consideration the current oversupply of stolen credit card details and E-banking logins aggregated through banker malware botnets, it shouldn't come as a surprise that [the price of stolen credit cards with complete owner's details is decreasing](#) . What shapes the price of a stolen credit card, what is the average price of this underground item, and how are the organized vendors of stolen credit card details embracing the Cybercrime-as-a-Service model?

"Credit card numbers fetch only \$2 or \$3 each on today's market, Dan Clements, head of [CardCops](#) , told Forbes.com. "Full profiles," data sets that include a credit card, mother's maiden name, date of birth, social security number and possibly an ATM PIN, command just \$10 apiece. Security giant Symantec says that bank accounts, credit cards and full profiles are the top three goods and services offered in the underground economy. Credit card data, they say, can trade for as little as 40 cents a card. By contrast, a decade ago, credit card information commanded as much as \$20 to \$30 per credit card, Clements says. That makes personal identity data almost a commodity: "They've come down on the curve a little bit, as it seems like more and more hackers and identity thieves have entered the market," he says."

Generalizing the average price for a stolen credit card with complete details for its owner, is a bit of an unrealistic attempt

to come up with verifiable evidence that the price is decreasing in general. How come? Basically, due to the nature of the underground marketplace, a potential buyer isn't aware of all the sellers of a particular good or a service, and is therefore doing business with who he perceives as the best vendor offering the best deal. Moreover, sampling different market propositions through the entire 2008, continues to indicate highly varying price ranges for the same item, whose chaotic percentage increases or decreases based on how much they "feel like" charging for the items, is making it harder to estimate the average price.

Anticipating the demand, and looking for more efficient ways to supply, the organized providers of stolen credit cards data have been embracing the Cybercrime-as-a-Service model during the entire year, coming up with do-it-yourself web services for purchasing the credit card details, where they monetize each and every aspect of the business model, by charging extra based on the number of lookups for a particular variable that they're missing. For instance, a sample web based service is charging the following prices for various verification services allowing a cybercriminal to restore the full identity of the credit card own, even through some of the details might be missing :

Mother's Maiden Name (\$3) Social Security Number (\$3) Date of Birth (\$0.5) Mother's Date of Birthday (\$1) Driver's License Number (\$8) Background Report (\$15) Credit Balance Report (25)

Here are the rules for using the value-adding, and extra charging service :

"1. Various lookup options are available (bins, zip, state, city, exp, sex). 2. Possibly to make a special order (rare countries, from 100 cvvs, negotiated price) 3.1 Cvvs can be checked right before sell at customers wish at additional price. 3.2 Invalid replacement in 72 hours time. 3.3 Replacement can be only in case of private checker service shows not APPROVED while check CCNUM+EXP. 3.4 VBS/MCSC can't be changed. 3.5 After 72 hours - ccs can't be replaced. 3.6 Results of checks at some checkers with code 05

DECLINE I do not accept, possible not compatibility of merchant and bank. 4. Cloned/Expired cards are excepted. 5. Service takes care of valid only, not their balance. It's available to sort cvvs by Classic/Gold/Platinum types, not a warranty of high balances. 6. Plz write me as correct as U can, coz sometimes I can't understand Ur slang. 7. Service can deny to process Ur request / to deal with You without explanation of reasons. 8. Seller is not a robot. He needs eat, sleep and live his own life. If I absent for a long time - Im not at the 'party', I have a serious reasons or went to another city/country. 9. For dummies - DO NOT CHANGE comment for WM transfer that I give to U. 10. Time spending online, can be changed, without notify of customers. 11. Not following service rules - can occur putting all consequences to a customer, and probably further black to customer. 12. Not allowed to flood my thread with posts "Where are U", "Why U not online", and "Im waiting for U". As consequence - ignore and U will be denied of service. 13. It is not allowed to intimidate service, to flood services icq / forum thread, to do hysterics. Who wants to solve their problem - can do It quietly. 14. Any service rule can be changed without notifying of customers."

And whereas the price for purchasing stolen credit card details is clearly decreasing in general, the value-added services and verification checks coming with it may gradually increase it in the long term. The bottom line, in a market segment with no indication of a monopolistic vendor of stolen credit cards, someone's stolen credit card is worth as much as the seller feels like charging for it, or based on his current price discount for bulk purchases.

Campaign Monitor hacked, accounts used for spamming | ZDNet

E-mail marketing software developer [Campaign Monitor warned users today of a server compromise](#) that took place during the weekend.

The compromise allowed the attackers to gain access to customer accounts, which they abused by importing their own lists of harvested emails in order to launch spam campaigns using the clean IP reputation of their servers. No credit card details have leaked, according to the company.

More info on the attack:

The main attack took place over this weekend, for a few hours on Saturday and Sunday and continuing into this week. We have up until now been gathering information so that we can contact you with accurate details, and also making sure we were stopping ongoing problems. We did not want to give you incomplete or misleading information. Right now we are still finding out more, but it is important you are all aware of the situation.

We are still actively working to get full detail on this, but essentially one of our servers was compromised, and that gave the hacker enough access to be able to get into a few customer accounts. We now know more, but don't want to publish any details as you can understand.

The incident reminds a similar one where [compromised university accounts](#) were used in the very same fashion. However, this tactic is fading due to a spammer's obsession with efficiency, which they're already achieving by using [automatically registered /compromised email accounts](#) , now representing close to [20% of the overall spam volume](#) .

Who's behind this attack? It's either a spammer opportunist, or unethical competition that went to great lengths in an attempt to have Campaign Monitor's servers blacklisted, which isn't happening based on their bounce rate monitoring.

The company has notified the owners of the affected accounts, and has commissioned an external security audit.

'Breaking: Lady Gaga Found Dead in Hotel Room' scam spreading on Facebook | ZDNet

Security researchers from Sophos have spotted [a currently circulating Facebook scam](#), enticing users into clicking on a bogus Lady Gaga themed video link.

Spamvertised as:

BREAKING: Lady Gaga Found Dead in Hotel Room. This is the most awful day in US history

Once the user clicks on the link, a redirection to a bogus BBC News page takes place. This is where the clickjacking takes place, once the user clicks on the "Play" button.

Users are advised to be extra vigilant when interacting with link found on Facebook.

Botnets committing click fraud observed | ZDNet

What's the current state of click fraud, and what tools and tactics do the people behind click fraud campaigns have in their

arsenal? A recently analyzed affiliate based network for using botnets to commit click fraud provides a timely assessment of the situation, and provides evidential facts on the internal success rate of such a consolidated botnet. Let's start with the current state of click fraud.

Is click fraud increasing or decreasing? According to ClickForensics, the click fraud rate has declined with 1& for Q1 of 2008, it still remains active at 27.8% for pay-per-click advertisements, with AdSense PPC model dominating the market. From their latest press release - "[Click Fraud Rate Drops to 16.3 Percent; Click Fraud Rate for Content NetworksLowers to 27.8 Percent](#) "

- The overall industry average click fraud rate was 16.3 percent for Q1 2008. That's down slightly from the 16.6 percent rate reported for Q4 2007 and up from the 14.8 percent click fraud rate reported for Q1 2007.
- The average click fraud rate of PPC advertisements appearing on search engine content networks, including Google AdSense and the Yahoo Publisher Network, was 27.8 percent. That's down from the 28.3 percent rate reported for Q4 2007 and up from the 21.9 percent average click fraud rate reported for Q1 2007.
- Q1 2008 click fraud traffic from botnets was 8 percent higher than click fraud traffic from botnets in Q4 2007.
- In Q1 2008, the greatest percentage of click fraud originating from countries outside North America came from Monaco (3.1 percent), Ghana (3.1 percent), and New Caledonia (2.4 percent).

As you can seen in Q1 of 2008, the click fraud traffic from botnets increased 8%, which from the perspective that I'll provide in the context of a sample output of such a botnet, will further verify this statement given the size of what looks like several botnets

consolidated into a single one while participating in an affiliation based program. Take a look at the following statistics distributed by the underground affiliate network to showcase the recent activity of its participants.

1,264,204 bots that did 3,095,194 searches and 537,764 clicks made a total revenue of \$5, 495, which when deducting percentage for the affiliate coordinating the campaigns, ends up with a profit of \$3,605 - this is a great example of greedy affiliate managers taking high commissions. The entire process of connecting owners of botnets who would only dedicate a single process for the click fraud, in between the rest of the malicious activities they'd be participating in between, is made possible through web traffic exchanges, like this one [covered by Brian Krebs](#) earlier this month :

Anyone who doubts that Internet click fraud has become a big money maker should take a look at a Russian Web site called Robotraff.com, which bills itself as "the first stock exchange of Web traffic." Set up a free account at Robotraff and you're ready to buy or sell Web traffic. Got 30,000 hacked personal computers under your thumb? Super! Now you can use those systems to generate a steady income just by pointing them at Web sites requested by a buyer. Or maybe you're just getting started and you can't be bothered to build your own army of hacked PCs the old-fashioned way? No problem! Now you can set up a Web site that tries to exploit Web browser or browser plug-in vulnerabilities and simply buy all the traffic you need.

Buying 100k of web site visitors, and having them redirected to a single URL, [where a cocktail of exploits is set up](#) by using the most popular web malware exploitation kits ([the Small Pack](#) , [Fire Pack](#) , [Mpack](#) , [Icepack](#) , or the [Nuclear Malware kit](#)), is exactly what such traffic exchanges get abused for, of course, in between click fraud. With [the underground market](#) dynamically evolving towards a service based economy, [the affiliation based market model](#) on a revenue sharing basis is a business model that's becoming largely anticipated by different parties as a perfect way to connect sellers and buyers, and of course, let the affiliate network cash-in by being the intermediary that connects them. What about the money trail in

the whole scammy ecosystem, as well as the current level of sophistication of the so called clickbots? [The Anatomy of Clickbot.A](#) should be considered a recommended bed time reading.

Bogus LinkedIn profiles serving malware | ZDNet

A currently active [malware campaign is taking advantage of bogus LinkedIn profiles](#) impersonating celebrities in an attempt to trick users into clicking on links serving bogus media players. LinkedIn is among the latest social networking services considered as a valuable asset in the arsenal of the blackhat SEO knowledgeable cybecriminal, simply because this approach works. For instance, Googling for "*Keri Russell nude* " or "*Brooke Hogan Naked pics* " you'll notice that the bogus profiles have already been indexed by Google and are appearing within the first 5/10 search results.

This is a proven tactic for acquiring search engine traffic which was most recently used in the [real-time syndication of hot Google Trends keywords](#) and using them as bogus content for the automatically generated bogus profiles using Microsoft's Live spaces. Approximately 70 to 80 bogus LinkedIn profiles appear to have been created within the past 24 hours, with LinkedIn's staff already removing some of them.

Go through related coverage of previous malware campaigns abusing legitimate services - ([Spammers targeting Bebo, generate thousands of bogus accounts](#) ; [Malware and spam attacks exploiting Picasa and ImageShack](#))

Upon several redirections a malware dropper (**TubePlayer.ver.6.20885.exe**) is served currently [detected by 10 AV vendors](#) as TrojanDownloader:Win32/Renos.gen!BB. Overall, the malware campaign is thankfully not taking advantage of any client-side vulnerabilities for the time being, leaving it up to the end user's vigilance -- if any if we're to exclude the [most abused infection vector for 2008](#) .

Bogus IQ test with destructive payload in the wild | ZDNet

Researchers from [ESET](#) and [BitDefender](#) have intercepted two destructive malware variants (*Win32/Zimuse.A*, *Win32/Zimuse.B/zipsetup.exe*), posing as an IQ test, and currently spreading in the wild.

Upon execution, the malware will attempt to spread through removable media using a time-based logic bomb, and overwrite the MBR ([Master Boot Record](#)) of all available drives after 40 days for variant A, and 20 days for variant B, making the host's data inaccessible.

More info on the malware:

The worm uses two ways to spread – either via embedding in legitimate websites, in the form of a self-unpacking ZIP file or as an IQ test program, or via Exchangeable media, such as USB devices. The fact that it relies on USB devices to propagate is responsible for its rapid dissemination, which is likely to increase even further.

To date, the worm's two variants - Win32/Zimuse.A and Win32/Zimuse.B differ in the method of spread and the timing of activation. While the A-variant needs 10 days to start spreading via USB devices, its B-variant needs only 7 days since infiltration. Moreover, the time needed for the execution of the destructive routine is shortened in the B-variant from the original 40 days to 20.

Moreover, once executed, the malware will also issue the following, typical for scareware/fake security software error message, in what appears to be an attempt by the malware authors to make the infected users contact the hosting provider of a particular site stating that it infected them with malware:

"System Defender - Kernel Error 0xC00000005

This problem is unambiguously caused by malicious contents in IP packers in transport layer from website: www.offroad-lm.szm.sk. To be patient, Windows Defender scan your hard drive(s) for bugs

caused by system incompatible code. To recovery of system press OK button. Wait to successfull end of scanning. Inform about this administrator on www.szm.sk and incriminated web site."

[BitDefender points out](#) that due to the digitally signed drivers in 64-bit versions of Windows Vista and Windows 7, the worm would fail to install. A [video demonstrating the infection](#) has been released, as well as a [Zimuse removal tool](#) , available for free download.

Bogus Google Files site earns revenue through premium rate SMS micro payments | ZDNet

Security researchers from AegisLab have stumbled upon a [bogus Google Search themed web site](#), offering downloads of multiple files in exchange for a SMS sent to a premium rate number.

The bogus web site offers downloads of music, programs, books, movies and adult content. This isn't the first time that scammers attempt to trick end and corporate users into interacting with their fraudulent campaigns. By brand-jacking a legitimate and trusted company's Web reputation, they successfully social engineer thousands of users into falling victims in them fraudulent schemes.

In 2008 and 2009 I profiled two [diversified domain portfolios of legitimate software](#) offered for download in case the user [sends a premium rate SMS](#) to the numbers provided. Back then, the campaign was managed by the bogus Interactive Brands Inc. company.

Thanks to the easy to obtain premium rate phone numbers, scammers continue actively looking for new ways to monetize content that's often available for free. Users are advised to avoid interacting with such services, as next to selling publicly obtainable software, they often harvest and resell the mobile phone numbers to [vendors of managed SMS spam services](#).

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Bogus Android apps lead to malware | ZDNet

Security researchers have detected a [new trojan horse targeting Android users](#) .

Using bogus Android apps, HongTouTou ([also known as ADRD trojan](#)) is using Android app marketplaces and forums to spread. The campaign is localized to Chinese; namely, it attempts to trick only Chinese speaking users.

Upon execution, the malware requests additional capabilities, next to sending the device's IMEI and IMSI to a remote host.

More info:

HongTouTou is included in repackaged apps made available through a variety of alternative app markets and forums targeting Chinese-speaking users. To date Lookout security researchers have identified fourteen separate instances of the HongTouTou Trojan repackaged in Android apps including RoboDefense (a well known game) and a variety of wallpaper apps.

See also:

[Man-in-the-middle attacks demoed on 4 smartphones](#)
[Researchers use smudge attack, identify Android passcodes 68 percent of the time](#)

What do you think is the biggest problem from a security perspective when it comes to mobile malware? The [flawed efficiency-driven Symbian OS](#) model? New [trust-chains relying on already authenticated user base](#) , or plain simple [social engineering attacks](#) .

Talkback.

Blizzard introducing two-factor authentication for WoW gamers | ZDNet

Password stealing malware targeting popular MMORPGs such as World of Warcraft for instance, has become so prevalent,

that video game developers are taking their authentication model a step further, by introducing two-factor authentication into play. And while marketable, is the new authentication layer actually useful in a real life situation? Depends. From [Blizzard's press release](#) :

"Blizzard Entertainment, Inc. today introduced an optional extra layer of security for World of Warcraft®, its award-winning massively multiplayer online role-playing game. Designed to attach to a keychain, the lightweight and waterproof Blizzard® Authenticator is an electronic device that generates a six-digit security code at the press of a button. This code is unique, valid only once, and active for a limited time; it must be provided along with the account name and password when signing in to the World of Warcraft account linked to it.

This optional security measure will be available for a cost of €6.00 at the 2008 Blizzard Entertainment Worldwide Invitational, which takes place June 28-29 in Paris, France. In addition, the Blizzard Authenticator will be made available for purchase via Blizzard Entertainment's European websites in the near future for a cost of €6.00 plus shipping.

"It's important to us that World of Warcraft offers a safe and enjoyable game environment," said Mike Morhaime, CEO and cofounder of Blizzard Entertainment. **"One aspect of that is helping players avoid account compromise, so we're pleased to make this additional layer of security available to them."**

Mike Morhaim's comment speaks for itself, since the two-factor authentication cannot prevent account compromise since a host that's already malware infected has already obtained and sent back the accounting data. What the two-factor authentication aims to achieve is ruin the efficient approach of abusing the hundreds of

thousands of already obtained passwords. And as always, it's usability versus security, since there are flaws allowing the bypass of the two-factor authentication.

For instance, the two-factor authentication is still optional, meaning that a great number of gamers wouldn't bother embracing it, and the higher the number of these, the more likely that the old fashioned management of hundreds of compromised accounts will continue in its current form. And with the number of people playing MMORPGs nowadays, this proportion of gamers that aren't using two-factor authentication would again remain vulnerable to the current types of password stealing malware. Timing is everything, and the worldwide launch of the token shouldn't have been announced before it was available to every gamer out there, since I anticipate "a wholesale summer promotion of stolen goods" before the compromised account holders associate their accounts with the Blizzard authenticator and start using it.

As for the future development of malware targeting WoW gamers, an [interesting propagation vector Storm Worm](#) used in early 2007 is the perfect analogy for what's to come. Next to using bogus Blogspot accounts, Storm Worm infected hosts were waiting for the end user to authenticate herself by filling in all the CAPTCHAs, a CAPTCHA that Storm Worm cannot and doesn't even need to break at legitimate blogs and forums. So once the end user authenticated herself, the now authenticated Storm Worm started posting links and blog posts redirecting to malware patiently waiting for the end user to provide Storm with access to its assets. Which is [exactly that we've seen seeing](#) on the [Ebanking malware](#) front [since 2007](#) , and what we'll be seeing in password stealers in the short term - adapting to the process and bypassing it entirely with the help of the malware infected gamer, a situation where SSL and two-factor authentication aren't an obstacle.

Since the stolen passwords are a commodity, but the authentication cannot be achieved remotely, password stealers for MMORPG's have the potential to mature into automated virtual asset stealers. Which is what they are after anyway.

BlackHole exploit kit experimenting with 'pseudo-random domains' feature | ZDNet

POST UPDATED, 27.06.2012.

In order to stay competitive within the cybercrime ecosystem, vendors of cybercrime-friendly services and tools need to constantly [innovate](#) and introduce the features requested by their users. What are some of the latest developments on the web malware exploitation kits' front?

According to [security researchers from Symantec](#), the author of the market leading BlackHole web malware exploitation kit is experimenting with a new feature offered as a trial to selected customers of his kit.

Based on their analysis, the kit's author is experimenting with a pseudo-random client-side exploits serving domain feature. Thankfully, the security researchers were able to decode the algorithm and are currently able to anticipate the exact domains to be registered at a future date, and consequently block access to them.

More details:

By changing the date passed to the function we can determine domains that will be used in future. All domains up to 7 August of this year have been registered and all currently resolve to the same IP address. The domains, all recently registered, use private registration, such as details of the registrant not published in WHOIS. So far we have seen a small but steady stream of compromised domains using this technique. This suggests that this is perhaps some kind of trial or test that could be expanded in future.

What is the kit's author aiming to achieve by introducing this feature? Automation which will inevitably results in the so called '[malicious economies of scale](#) ', the two key features of a web malware exploitation kit.

In the past, the [BlackHole exploit kit](#) relied on a managed script crypting service, periodically updating the client-side exploits serving domains. It's interesting to observe the newest feature of the kit, in the context of automation, as it indicates that the kit's author is clearly interested in maintaining his market leader share by persistently introducing new features and exploits.

[BlackHole exploit kit's](#) successful infection rates are high primarily due to the fact that the kit is exploitation commonly found client-side vulnerabilities in third-party software and browser plugins.

Users are advised to ensure that they're not using [outdated third-party software](#) and [browser plugins](#).

UPDATE: [According to researchers from StopMalvertising.com](#) , the pseudo-random domains feature is not exclusively tied to the BlackHole exploit kit as Symantec originally states. The feature is also found on multiple compromised URIs, and introduces a new domain every 12 hours. Apparently, certain cybercriminals have obtained the source code of the feature, and are currently experimenting with it, using the BlackHole exploit kit as a method of choice for serving client-side exploits.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

BlackBerry users targeted with malware-serving email campaign | ZDNet

Security researchers from Websense, have intercepted a [currently spamvertised malicious campaign](#), attempting to trick BlackBerry users into downloading and executing the malicious .zip archive.

The archive with [MD5: 9a01293b87b058619d55b8d4d12f2a8e](#) is currently detected by 27 out of 42 antivirus scanners as Backdoor.Win32.Androm.gj; Worm:Win32/Gamarue.l.

On a periodic basis, cybercriminals mass mail millions of emails impersonating multiple brands in an attempt to target as many market segments as possible. Thanks to the publicly available [DIY email harvesting tools](#), and managed [databases of already harvested](#) millions of [segmented email addressess](#), cybercriminals are at a unique position to reach out to millions of Internet users in a matter of hours.

We're definitely going to see more systematic abuse of well known and trusted brands, in an attempt by the cybercriminals to socially engineer end and corporate users into interacting with their campaigns.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Black market for zero day vulnerabilities still thriving | ZDNet

One would assume that popular sources for zero day vulnerabilities+Poc's such as Full-Disclosure, Bugtraq or Milw0rm are the primary sources for obtaining responsibly or irresponsibly released flaws. They'd be wrong. The black market for zero day vulnerabilities and the concept of over-the-counter (OTC) trade of zero day flaws, has been gradually developing itself through the last couple of years.

Let's take a brief retrospective of the black market for zero day vulnerabilities, and review a recently launched underground shop for zero day vulnerabilities, currently offering 15 zero day vulnerabilities affecting popular web applications in order to execute successful XSS or SQL injection attacks, with prices ranging from \$10 to \$300.

Back in 2005, a bid for a zero day [vulnerability affecting Microsoft's Office Excel](#) was posted on Ebay prompting mass media outbreak on the potential of rewarding security researchers for their research. It didn't take long before [a zero day vulnerabilities cash bubble](#) started to form, with legitimate sellers and cybercriminals over hyping the seriousness of their discoveries. Around December, 2005, the first publicly disclosed case of underground market trade of zero day vulnerabilities took place when it became evident that the the infamous [Windows Metafile vulnerability](#) (WMF vulnerability) [has been sold for \\$4,000](#) :

"It seems most likely that the vulnerability was detected by an unnamed person around 1st December 2005, give or take a few days. It took a few days for the exploit enabling random code to be executed on the victim machine to be developed. Around the middle of December, this exploit could be bought from a number of specialized sites. It seems that two or three competing hacker groups from Russian were selling this exploit for \$4,000. Interestingly, the groups don't seem to have understood the exact nature of the vulnerability. One of the purchasers of the exploit is

involved in the criminal adware/ spyware business, and it seems likely that this was how the exploit became public."

Interestingly, the authors of the then popular WebAttacker DIY web exploitation kit started conducting basic market research on the potential of this market, by featuring a survey asking their visitors how much they would be willing to pay for a zero day vulnerability. The results out of 155 votes indicated that 40% of the potential buyers were willing to pay between \$100 and \$300, with 14.19% answering that they code their own zero day exploits and another 17% stating that they obtain them for free.

It didn't take long before the underground market model materialized in the face of the International Exploits Shop, among the first underground offerings of a web malware exploitation kit featuring a multitude of client-side vulnerabilities, next to two zero day flaws back in 2006. And whereas the shop quickly disappeared, the concept always remained there.

In times when [legitimate online auctions for zero day vulnerabilities](#) are admitting that the market model they've introduced is far ahead of its time, their underground alternatives are thriving. Launched in early

August, this web based shop is the latest attempt to utilize a black market model for zero day vulnerabilities.

Here's a translated introduction to the exploits shop :

"We present you the private exploits shop targeting PHP-applications (Content Management Systems, Guest books, forums, chat rooms, statistics and any other scripts). Our store will be constantly updated so you can expect to find the exploit you were looking for at any given time. If it doesn't you will still be able to request such a vulnerability for a web application of your choice, and our team will provide with you the necessary PoC's and tools to start using it. All exploits are written solely to our command, meaning you're not going to find them anywhere else on the Internet.

Each exploit is accompanied by information on the approximate number of sites running the vulnerable application in Google, the language the exploit is written in, and price. We also have a forum

where you can place an order, discuss, complain, express an opinion or ask a question about the exploit purchased. All exploits have a user-friendly Web interface, possibly in the future we'll be releasing win32 console exploits. There are also technical support, patiently waiting for requests from users who have a problem using the exploit. We also conduct audits, security services, tests for entry (this service will be available by the end of August this year).

Watch our virtual merchandise, and if not today perhaps tomorrow you'll find what you're looking for."

What's particularly interesting about the service is the major shift towards exploitation of web applications in order to facilitate massive SQL injection attacks compared to previously known and analyzed services focusing exclusively on client-side vulnerabilities.

As always, you have a pure cybercrime market proposition pitched as a security service. The e-shop is not only offering proof of concept exploits to demonstrate the vulnerabilities, but also, easy to use web based applications for exploitation.

Moreover, this pseudo responsible positioning is flawed right from very beginning since the service administrators have done their homework and are also offering stats from basic search engines reconnaissance -- [Google dorks](#) -- so that potential buyers can easily measure the impact of the flaw that they're purchasing. These very same vulnerabilities would later on be abused for blackhat search engine optimization, and injection of malicious scripts redirecting to live exploit serving URLs. Here's their ethical pen-testing pitch :

"Our team is reviewing source code software and finding bugs in the programming, leading to critical consequences and employees of security systems. Thus, we are pleased to offer you the results of their analysis of popular (or little) systems. The results of our study are presented in the form of finished applications in languages php / perl, which aim - to demonstrate the vulnerability of the system to further assist in their neutralization. If you're going to use our software for other purposes than penetration testing, the administration does not take responsibility for your actions.

We also take orders for individual study of your source code, security auditing of servers and sites (penetration tests). Orders for

such services are taken at the forum, and the price purely individual and dealt with each customer individually (mainly depends on the number and type of vulnerabilities discovered, as well as the number of code)."

Which products are they targeting? Currently offered zero days affect multiple versions of the following web applications :

- All versions of PHP Fusion - WHMCompleteSolution - PHP Nuke
- PunBB - Tiki Wiki - BMForum - Invision Power Board - YaBB - PunBB - e170 Plugin Calendar - vBulletin v3.6 + ICQ Mod - vBulletin v3.6 + GVideo Mod - vBulletin v3.6 + Youtube Mod - vBulletin v3.6 + LJ Mod - Zen Cart

The most expensive is the \$300 SQL injection flaw affecting all versions of PHP Fusion, which can be exploited on a large scale since there are over 2.5 million instances of it on the web, and even if the stats are conservative this hit list building approach through search engines reconnaissance has always been there, with the most recent proof of its usability were the massive SQL injections attacks.

Next to their current inventory, the service is also offering zero day vulnerabilities on demand charging the following prices :

- "- Remotely upload shell - \$120 - Remote file inclusion on request - \$100 - Remote SQL injection - \$70 - Passive and Active XSS for \$10 and \$40 respectively"

This overall shift from client-side vulnerabilities to web applications based ones is taking place due to the increasing demand for techniques allowing the easy hijacking of traffic from legitimate web sites, which is where these web application vulnerabilities fit in. Once they acquire the traffic by exploiting them, they would ultimately redirect it to malware and exploits serving domains taking advantage of [outdated but unpatched on a large scale client-side vulnerabilities](#) . It's all a matter of perspective, and the people behind this particular e-shop for zero days are taking the pragmatic one by offering the right product for the right moment.

Bill O'Reilly's web site hacked, attackers release personal details of users | ZDNet

In what is slowly turning into an endless loop of hacktivism activities, [Bill O'Reilly's BillOreilly.com has been compromised during the weekend](#), with personal details including passwords in plain text for 205 of the site's members already leaking across Internet forums, as a response to [his remarks regarding Wikileaks](#) as a "one of those despicable, slimy, scummy websites" which [recently published](#) private information of [Sarah Palin's private email](#).

On Friday, [Wikileaks issued](#) the following press release :

"Fox News demagogue, Bill O'Reilly, has been hacked and the details passed to Wikileaks. Wikileaks has been informed the hack was a response to the pundit's scurrilous attacks over the Sarah Palin's email story--including on Wikileaks and other members of the press, Hacktivists, thumbing their noses at the pundit, took control of O'Reilly's main site, BillOReilly.com. According to our source, the security protecting O'Reilly's site and subscribers was "non-existent".

The following image, submitted to Wikileaks and confirmed by Wikileaks staff, offers proof of the hack. The image, clearly obtained from BillOreilly.com's administrative interface, shows a detailed list -- including passwords -- of BillOreilly.com subscribers. Although Wikileaks has only released one page, it must be assumed that Bill O'Reilly's entire subscriber list is, as of now, in the public domain."

How did they do it "this time"?

According to the article at Wikileaks, the hacktivists seem to have been brute forcing the URL for the administration panel, and once successfully finding it, access the unencrypted data :

"According to Marston, the hackers were able to access the list by trying a large number of variations of the website's administrative URL. He said all affected members have received an email and a phone call informing them of the breach and urging them to change their password. The site has since been completely locked down, Marston said."

Moreover, it's also worth pointing out that the passwords were stored unencrypted, evidence of the practice can also be seen within the screenshots of the admin panel. As far as the website's administrative URL is concerned, it has since been changed [once it leaked online](#) ([**w3.billoreilly.com/pg/jsp/admin/managecustomers/newpremiummembers.jsp**](http://w3.billoreilly.com/pg/jsp/admin/managecustomers/newpremiummembers.jsp)), which isn't excluding the opportunity for abuse of the subscribers email addresses in spear phishing attacks, "for starters" since some of the users have already admitted of [using the same password at different web sites](#) , including PayPal.

The impact of the breach, and the measures taken to notify the victims [according to the site](#) :

"The BillOReilly.com site experienced a minor hacking incident on Friday, September 19th, 2008.

**** ALL CREDIT CARD INFORMATION FOR EVERY MEMBER IS SAFE ** NO MEMBERS WHO JOINED BEFORE WEDNESDAY, SEPTEMBER 14th, 2008 WERE AFFECTED AT ALL. ** 205 new Premium Members who signed up last week had their name, hometown, email address, & BillOReilly.com password stolen. ** We have contacted those 205 members by email and telephone. ** We are working with the proper authorities to track down the perpetrators. "**

Another personal message issued by Bill O'Reilly regarding the process of [tracking down the "perpetrators"](#) was posted on Sunday :

"The FBI and Secret Service are close to indicting some of the perpetrators and we will keep you posted when the arrests are made. All premium members receive the full backing of our legal team and if anyone is hassled in the least, please inform us immediately. In the latest case, no proprietary information was obtained by hackers and we have safeguards in place to protect everyone who does business with us.

Rest assured that we are on this. Our defense of Sarah Palin has led some criminals to attempt to disrupt our enterprise. At this moment federal authorities and our attorneys are compiling information against these people. Again, if any person is bothered in any way - please let us know. We stand behind our products but,

most importantly, we stand behind you. We'll get the bad guys. Count on it.

Bill O'Reilly 9/21/08"

Who's claimed responsibility? [4chan members planning at Ebaumsworld](#) using "secret words" :

"According to my source this is a common tactic among the secret hacking group hidden amongst the users of ebaumsworld. he states "yeah we will start planning on 4chan so ebaums doesnt get in trouble...we use secret words and stuff to let the others know who we are" when i asked why he was telling me all this he said "man this has just gone too far.. at first it was a joke then we found out that the same usernames and passwords worked for those peoples paypal accounts and im afraid of what they will do."

It appears that the "forum fraction" is also planning a [DDoS attack against BillOreilly.com according to this interview](#) , which wouldn't be the first time [the site has been under DDoS attack](#) , and definitely not the last. From an analyst's perspective, [nation2nation hacktivism conflicts](#) always provide the best and most accurate understanding of a particular's country's capabilities into this space, compared to hacktivism actions basically sticking to the standard practices as DDoS attacks, which just like any tip of the iceberg receive most of the attention due to the ease of measuring their impact next to the rest of the hacktivism tactics used.

The bottom line - good time to point out why you shouldn't use the same password on different web services, and that the big picture having to do with Wikileaks vision of a little less secrecy, and a little bit more transparency, ultimately better serves the world and gives power to the people whose collective consciousness, if not brainwashed, is supposed to be shaping the way we live.

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/> and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back these settings

CLOSE

Hotmail's new security features vs Gmail's old security features | ZDNet

Microsoft's revamped Hotmail, set to be [rolled out in mid-summer according to the company's](#) press release, [introduces several new security features](#), among which are full-session SSL, visual indication for trusted email senders, and improved password recovery mechanisms.

Let's review them, their applicability to today's cyber threatscape, and compare them to Gmail's currently available security features.

Trusted senders . With the new Hotmail, we help you to visually identify trusted senders in your inbox, particularly banks and other senders most commonly impersonated in phishing scams, by putting safety logos next to those senders who we recognize as legitimate.

Full-session SSL - In addition to providing SSL encryption of credentials at login for all accounts, the new Hotmail will soon support the option to maintain SSL encryption between you and Microsoft servers during your entire Hotmail session.

Single-use codes - This new security feature is designed to further help protect you by giving you the option to ask Hotmail to SMS to you a one-time temporary password if you'd prefer not to use your regular password when logging into Hotmail on public computers that could potentially harbor key logging malware that could steal your password, such as those sometimes found in internet cafes and airports.

Account security information - The new security platform elements we've built up around Hotmail now enable you to use your cell phone or other items as proof of account ownership. For example, if you lose your password or, worse, if your account gets compromised, we can now send you an account recapture code via an SMS message or enable you to regain access to your account.

Playing catch up from a security perspective in the free email market segment -- sorry Microsoft -- offers unique business

development opportunities, that if well executed can position the follower as the market (segment) leader, at least for a while.

And although the introduction of safety logos for over [100 banks/financial institutions](#), is a great idea, since it would help less technically sophisticated Hotmail users spot the fraudulent emails more easily, both, trusted senders ([July, 2009](#)), full-session SSL ([July, 2008](#)), and SMS-based password recovery, have been available to Gmail users for a while.

In order to fully seize the marketing momentum, market (segment) followers are supposed to set new benchmarks, and do their best to avoid "me-too" product feature catch-up based strategies. Interestingly, Microsoft appears to have achieved it by introducing the **SMS-based single sign in codes**.

In comparison, Gmail only has a [password recovery option via SMS](#), introduced in June, 2009. Here's a chronology of the introduced security features at Google's Gmail over the years:

2004 - [Gmail Begins Signing Email with DomainKeys](#) **2008** - [Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails](#) **2008** - [Making security easier \(choice for always on SSL\)](#) **2008** - [Remote sign out and info to help you protect your Gmail account](#) **2009** - [Google Account Recovery via SMS](#) **2009** - [The super-trustworthy, anti-phishing key \(visual Trusted Senders confirmation\)](#) **2010** - [Default https access for Gmail](#) **2010** - [Security alerts for Gmail](#)

Which are the unique features offered exclusively by only one of the email providers?

Basically, if it wasn't for **Hotmail's upcoming single-use codes**, their whole campaign would have been an embarrassing catch up marathon with Google's Gmail. **Gmail's [security alerts](#) feature**, however, still differentiates by emphasizing on the real-time notification for a compromise that's currently taking place.

Is there a particular security feature that both, Microsoft and Google failed to implement so far? Has the time come for both companies to acknowledge the existence of public key cryptography

within their settings interface? What about the availability of [disposable/temporary email accounts](#) generation feature?

Moreover, how user-friendly was your experience with both email providers, in cases of an account compromise? With do it yourself account import and export options, is the increased security offered by a particular provider, enough for you to migrate there?

Talkback, and share you opinion.

'Hot Lesbian Video - Rihanna and Hayden Panettiere' scam on Facebook leads to Mac malware | ZDNet

Researchers from Sophos have [intercepted a currently ongoing Facebook scam](#) which exposes users to [Mac scareware](#).

Spamadvertised as:

one more stolen home porn video ;) Rihanna and Hayden Panettiere
Hot Lesbian Video - Rihanna And Hayden Panettiere!!
Rihanna And Hayden Panettiere !!! Private Lesbian HOT Sex Tape stolen from home archive of Rihanna!

Upon clicking on the link, users are exposed to a fake scanning window, which is actually [MAC OS X scareware](#) variant currently detected as OSX/FakeAV-DWK, OSX/FakeAV-DWN, OSX/FakeAvDI-A and OSX/FakeAVZp-C.

Users are advised to be extra vigilant when interacting with Facebook links, even those distributed by trusted friends, and take advantage of the [anti-clickjacking features](#) offered by the NoScript Firefox add-on.

HD Moore pwned with his own DNS exploit, vulnerable AT&T DNS servers to blame | ZDNet

A week after [J\)ruid and HD Moore release part 2 of DNS exploit](#) , HD Moore's company [BreakingPoint has suffered](#) a traffic

redirection to a rogue Google site, thanks to the [already_poisoned cache at AT&T servers](#) to which his company was [forwarding DNS traffic](#) :

"It happened on Tuesday morning, when Moore's company, BreakingPoint had some of its Internet traffic redirected to a fake Google page that was being run by a scammer. According to Moore, the hacker was able to do this by launching what's known as a cache poisoning attack on a DNS server on AT&T's network that was serving the Austin, Texas area. One of BreakingPoint's servers was forwarding DNS (Domain Name System) traffic to the AT&T server, so when it was compromised, so was HD Moore's company. When Moore tried to visit Google.com, he was actually redirected to a fake page that served up a Google page in one HTML frame along with three other pages designed to automatically click on advertisements."

Moreover, last month, before the latest [DNS cache poisoning vulnerability and exploits started taking place](#) , Metasploit Project's site was [temporarily hijacked through ARP poisoning](#) , perfectly demonstrating that old-fashioned DNS attacks remain intact.

UPDATE: [HD Moore's explanation of the situation, and the impact of the attack that took place](#) :

"Most of the facts of the article are correct. I have no problem detailing the attack, how it worked, and how we detected and resolved it. I am careful about the wording, because I want to be clear that while this type of attack can be serious, in this case it was a five minute annoyance that was designed as a revenue generator for the folks who launched it (click-through advertisement revenue).

No systems were been compromised, no data was stolen, and most importantly, the target of the attack was the ISP, not the company that I work for. Stating that my company was "compromised" leads the reader to believe that there was some sort of security breach, which is reinforced by the fabricated quote."

Haiti earthquake themed blackhat SEO campaigns serving scareware | ZDNet

Cybercriminals quickly mobilized following the news of a [massive earthquake that hit Haiti](#) on Tuesday, by introducing several hundred [compromised domains embedded with bogus blackhat seo](#) (search engine optimization) content related to Red Cross donations and general Haiti earthquake relief information.

The sites are [already appearing within the first 10 search results on Google](#), and upon clicking on them the user is redirected to one of the most profitable monetization tactic ([FBI: Scareware distributors stole \\$150M](#)) that scammers use these days - [scareware also known as rogueware](#).

Naturally, the blackhat SEO campaigns are only the tip of the iceberg. Here's what else to look for, and how to make sure you're donating money to the right organization.

What's particularly interesting about the blackhat SEO campaign serving scareware ([Setup_2022.exe](#); [install.exe](#)), is that a huge percentage of the sites are hosted within the network of Heart Shared hosting ([heartinternet.co.uk](#)), indicating some some of automatic exploitation of its customers.

The same practice of relying on compromised legitimate domains within a particular ISP was also evident in blackhat SEO campaigns that were analyzed over the last couple of months.

For

instance, not only was the same practice used to affect over a million web sites ([Thousands of web sites compromised, redirect to scareware](#)) in November, 2009, but also [the campaign itself was traced back to the Koobface gang](#), which is clearly involved in fraudulent activities going beyond the Koobface botnet.

Different fraudulent groups either multitask, or cover a specific fraud segment exclusively. According to Symantec, [spam campaigns impersonating the British Red Cross](#) are already in circulation,

requesting Western Union payments to support the victims of the earthquake. Anticipating the upcoming flood of earthquake relief scams, [the FBI has released the following tips](#) in order to raise more awareness:

Do not respond to any unsolicited (spam) incoming e-mails, including clicking links contained within those messages.

Be skeptical of individuals representing themselves as surviving victims or officials asking for donations via e-mail or social networking sites.

Verify the legitimacy of nonprofit organizations by utilizing various Internet-based resources that may assist in confirming the group's existence and its nonprofit status rather than following a purported link to the site.

Be cautious of e-mails that claim to show pictures of the disaster areas in attached files because the files may contain viruses. Only open attachments from known senders.

Make contributions directly to known organizations rather than relying on others to make the donation on your behalf to ensure contributions are received and used for intended purposes.

Do not give your personal or financial information to anyone who solicits contributions: Providing such information may compromise your identity and make you vulnerable to identity theft.

If you want to donate money to the real organizations, consider going through [Google's Support Disaster Relief in Haiti campaign page](#).

Hacking group from Nepal posts 10,000 stolen Facebook accounts online | ZDNet

A hacking group from Nepal known as [TeamSwaStika](#), has published 10,000 stolen Facebook accounts on Pastebin for everyone to see and take advantage of.

The group appears to have obtained the stolen accounting data, through either phishing, or data mining malware-infected hosts for Facebook credentials. Another alternative would be that they have purchased the cache containing the stolen credentials from a specific service reselling accounting data, as these services are quite popular within the cybercrime ecosystem nowadays.

As a precaution, Facebook users are advised to periodically change their passwords from a malware-free host.

Hackers hijack DNS records of high profile New Zealand sites | ZDNet

Remember the DNS hijackings of such [high profile sites](#) such as [Comcast](#) , [Photobucket](#) , and [ICANN/IANA](#) domains that were taking place last year? Similar incidents are still happening.

Today, a web site defacement group known as "The Peace Crew" has successfully [hijacked the DNS records for high profile New Zealand web sites](#) , through what Zone-H claims to be a SQL injection at New Zealand's based registrar Domainz.net, in order to redirect the visitors to a defaced page featuring the infamous Bill Gates pieing photo, as well as anti-war messages.

[The mass defacement](#) affected major Microsoft sites in New Zealand including **WindowsLive.co.nz** , **MSN.co.nz** , **Microsoft.co.nz** , **Hotmail.co.nz** , **Live.co.nz** next to **HSBC.co.nz** , **Sony.co.nz** , **Coca-Cola.co.nz** , **Xerox.co.nz** , **Fanta.co.nz** , **F-Secure.co.nz** and **BitDefender.co.nz** .

Here's Microsoft's comment:

[According to NZHerald](#) :

"MSN have responded by issuing a short statement from MSN business manager Liz Fraser this afternoon. "The cause of this discrepancy has been identified and we are currently working with our Microsoft technology and security teams in the US to resolve the matter as quickly as possible today. "We apologise for any inconvenience this may have caused," the statement said."

Once control to the domain registrar's web panel was obtained, members of the Peace Crew used [fatih1.turkguvenligi .info](#) and [fatih2.turkguvenligi .info](#) as [primary DNS servers](#) delivering the defaced pages, and making it look like the sites themselves have been compromised.

Go through related hacktivism/web site defacement cases: [Thousands of Israeli web sites under attack](#) ; [Pro-Serbian hacktivists attacking Albanian web sites](#) ; [Hundreds of Dutch web sites hacked](#)

[by Islamic hackers](#) ; [300 Lithuanian sites hacked by Russian hackers](#)
; [Chinese hackers deface the Russian Consulate in Shanghai](#) ;
[China detains web site defacer spreading earthquake rumors](#)

The group is not new on the defacement scene, in fact one of its members has been keeping himself pretty busy during this month by having already [defaced thirteen web servers belonging to NASA](#) , using the same template.

GPU-Accelerated Wi-Fi password cracking goes mainstream | ZDNet

No weak password can survive a GPU-accelerated password recovery attack. Last week's released [Wireless Security Auditor](#) is prone to shorter the time it takes for a network administrator to pen-test the strength of the WPA/WPA2-PSK passwords used on the wireless network. Its core functionality of shortening the wireless password recovery time up to a hundred times based on the GPU used, is naturally going to empower unethical wardrivers with the ability to easily guess the no longer considered secure 8 character passwords.

What's particularly interesting about the [Wireless Security Auditor](#) is that it attempts to accomplish the password recovery in an offline/stealth mode, instead of the noisy direct router brute forcing approach :

"Elcomsoft Wireless Security Auditor works completely in off-line, undetectable by the Wi-Fi network being probed, by analyzing a dump of network communications in order to attempt to retrieve the original WPA/WPA2-PSK passwords in plain text. Elcomsoft Wireless Security Auditor requires a valid log of wireless communications in standard tcpdumptcpdump. The tcpdumptcpdump format is supported by all commercial Wi-Fi sniffers. In order to audit your wireless network, at least one handshake packet must be present in the tcpdump file."

Meanwhile, [pen-testing companies](#) have once again urged IT managers and end users to go beyond the 8 character password strength myth, and anticipate the risks posed by the increasingly efficient password recovery solutions hitting the market :

"David Hobson said: "It's a wake-up call to IT managers, pure and simple. IT managers should now move to 12 and even 16 character keys as a matter of urgency. It's not very user-friendly, but the potential consequences of staying with eight character keys do not bear thinking about."

As [previously discussed](#) , best practices wake-up calls remains largely ignored prompting radical solutions in countries like India for instance, which recently announced that a [Wardriving police unit](#) will be locating [insecure wireless networks](#) and notifying the owners in order to "prevent the commission of a cognizable offense".

Google's CAPTCHA experiment and the human factor | ZDNet

Any research is prone to irrelevance if it starts with the wrong research questions, takes the wrong perspective, or in this case, [attempts to fight the wrong enemy](#) - automated bots attempting to recognize CAPTCHAs.

Researchers at Google recently released a paper detailing a new CAPTCHA system consisting of correct image rotation ([Socially Adjusted CAPTCHAs](#)) whose main purpose is to make it easier for humans, and much harder for bots to recognize them. But with the emphasis of this and many other research papers on "bots vs CAPTCHAs", the research excludes a growing trend to which the new approach -- if implemented -- would actually make the new CAPTCHA much more efficiently abused than the previous one.

How come? Despite the persistent attempts by malware infected hosts to recognize CAPTCHAs, at the end of the day, a data entry team capable of [solving 200,000 CAPTCHAs and charging \\$2 per 1000 entries ultimately drives the CAPTCHA solving economy](#).

A lot has changed since the factual research detailing "[Inside India's CAPTCHA solving economy](#)." was published last year.

Following their improved recognition rates -- in case you remember you have to pass a CAPTCHA solving speed test in order to become a qualified CAPTCHA solver -- the vendors of these services consisting primarily of boutique shops and a few consolidated ones, have gone mainstream to the point where Russian based CAPTCHA solving services are outsourcing the process to Indian workers and charge their customers more than the pay to their Indian colleagues.

In February this year, a novel approach was introduced by a Russian boutique vendor of CAPTCHA solving services - a [community-driven revenue sharing scheme for CAPTCHA breaking](#). The concept is mimicking reCAPTCHAs ease of implementation and ubiquity, but with a mean perspective in mind. It allows webmasters

to not only implement CAPTCHA solving forms at their registration pages, but is offering idle forum/community members the opportunity to solve CAPTCHA and earn revenue in the process, with the successfully solved CAPTCHAs fed into their system fulfilling yet another bulk request for bogus account registration.

Go through related CAPTCHA posts: [Microsoft's CAPTCHA successfully broken](#) ; [Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers](#) ; [Spammers attacking Microsoft's CAPTCHA -- again](#) ; [Spam coming from free email providers increasing](#) ; [Gmail, Yahoo and Hotmail systematically abused by spammers](#)

Perhaps even more disturbing is the fact that these vendors are naturally Web 2.0 aware, and are clearly working with some of the most popular vendors of blackhat search engine optimization and automatic account registration/spamming tools by offering them the capability to empower their customers with CAPTCHA solving capabilities through API keys.

A practical example of how these human networks efficiently exploit CAPTCHA systems originally designed to fight bots, and facilitate cybercrime in the process, is the social networking worm Koobface ([Koobface Facebook worm still spreading](#) ; [Dissecting the Latest Koobface Facebook Campaign](#) ; [Dissecting the Koobface Worm's December Campaign](#) ; [The Koobface Gang Mixing Social Engineering Vectors](#)).

Koobface is eating every social network's internal CAPTCHA barrier for breakfast not because the Koobface gang is taking advantage of CAPTCHA recognition algorithm, but because it's relying on CAPTCHA solving services. [Sergei Shevchenko at ThreatExpert](#) demonstrated the process in December, 2008, and pointed out that :

"In the real test, Facebook.com asked the Koobface to resolve the CAPTCHA image that reads "suffer accorn" - this image was pretty noisy for image recognition algorithms to resolve it successfully. But Koobface does not attempt to resolve it by itself. It submits this image to its C&C server. The server replies correct answer in about 34 seconds. Once the answer is received, Koobface submits the

message via Facebook's compromised account including correct CAPTCHA answer."

With [human networks and bots clearly converging](#) (see graph), Sergei also discussed a very pragmatic solution on defeating Koobface back then - injecting a large number of successfully accepted CAPTCHA images to Koobface's command and control server, have them resolved by the CAPTCHA solving vendor, and the bill sent to the Koobface gang :

"Detailed analysis of traffic between Koobface and its command-and-control server allowed tapping into its communication channel and injecting various CAPTCHA images in it to assess response time and accuracy. The results are astonishing – the remote site resolved them all.

But here is a twist: uploading a large number of random CAPTCHA images into its communication channel will load its processing capacity, potentially up to a denial-of-service point. Well, if not that far, then at least it could potentially harm its business model, considering that the cost of resolving all those injected images would eventually be paid by the Koobface gang."

The ongoing arms race is not between bots vs CAPTCHAs, its between human networks efficiently exploiting networks aimed to originally distinguish between humans and bots. No CAPTCHA can survive a human, since it was originally meant to be recognized by one, and therefore making it easier to be recognized by humans like in Google's recent experiment, ultimately makes it easier for the CAPTCHA solving economy to scale.

CAPTCHA is in pain, humans are slowly killing it not bots. What do you think?

Google Video search results poisoned to serve malware | ZDNet

From the real-time syndication of hot [Google Trends keywords](#) , maintaining [AdWords campaigns](#) , to the plain simple blackhat search engine optimization tactics, cybercriminals are constantly looking for new ways to acquire traffic by enjoying the clean reputation of each and every Web 2.0 property. From [LinkedIn](#) , [Bebo](#) , [Picasa and ImageShack](#) , to [Twitter](#) , everyone's targeted efficiently using automated account registration tools.

During the last couple of days, a single group involved in a countless number of blackhat SEO campaigns across the Web, started massively targeting Google Video with a campaign that has already managed to hijack approximately 400,000 search queries in order to trick users into visiting a bogus and malware serving ([W32/AutoTDSS.BNA!worm](#)) adult web site.

Here's how the campaign works, and how they're attempting to cloak it from the eyes of security researchers.

What's particularly interesting about this campaign relying entirely on Google Video traffic to flourish, is that instead of sticking to the adult content in their keywords inventory, the cybercriminals have been in fact syndicating legitimate YouTube video titles from a variety of topics. Therefore, the number of legitimate videos used is proportional to the comprehensiveness of the campaign, in this case, over 400,000 search queries, a number that is increasing in real-time since they keep having their bogus content crawled by Google Video.

Moreover, based on the fact that they maintain a portfolio of 21 publisher domains with bogus and non-existent video content currently crawled, a simple tactic that they're using could entirely hijack a search query at Google Video. How come? By simply duplicating the content on their publisher domains, the top 5 search results for a particular video can be easily served from any of the 21

publisher domains, making it look like different sites have the same content.

The search engine results poisoning works as follows. Upon clicking, a Google Video user coming across to any content from any of their 21 publisher domains, is taken to a single redirection point (**porncowboys .net/continue.php**), then to the well known adult site template abused by cybercriminals (**xfucked .org/video.php?genre=babes&id=7375**), where the user is told that *"Your Flash Version is too old. Your browser cannot play this file. Click "OK" to download and install update for Flash Video Player "* and the malware is served if he's tricked into it (**trackgame .net/download/FlashPlayer.v3.181.exe**).

The cybercriminals are also taking advantage of a well known evasive technique - http referer checking or "cloaked maliciousness. For instance, the malware redirection to the fake flash player is only served if the potential victim is coming from Google Video. If a researcher is basically browsing around the content of their sites, the legitimate YouTube videos are legitimately syndicated. Excluding this case, it's worth pointing out that on the majority of occasions cybercriminals do not fully take advantage of the evasive features available within the traffic management kits they use behind the campaigns, making their campaigns easier for analyzing.

Google's Security Team has been notified and action is expected to be taken anytime now.

Google tops comparative review of malicious search results | ZDNet

According to a newly released [report by Barracuda Labs](#), based on a two-month study reviewing more than 25,000 trending topics and 5.5 million search results, Google remains the most popular search engine used by malicious attackers, relying on poisoned keywords.

The company, which also sampled [Yahoo Search](#), [Bing](#), and [Twitter](#), contributes Google's leading position to the fact that Google remains the market share leader in online search, and consequently the most targeted search engine.

Key highlights of the study:

Overall, Google takes the crown for malware distribution – turning up more than twice the amount of malware as Bing, Twitter and Yahoo! combined when searches on popular trending topics were performed. Google presents at 69 percent; Yahoo! at 18 percent; Bing at 12 percent; and Twitter at one percent.

The average amount of time for a trending topic to appear on one of the major search engines after appearing on Twitter varies tremendously: 1.2 days for Google, 4.3 days for Bing, and 4.8 days for Yahoo!

Over half of the malware found was between the hours of 4:00 a.m. and 10:00 a.m. GMT. The top 10 terms used by malware distributors include the name of a NFL player, three actresses, a Playboy Playmate and a college student who faked his way into Harvard.

Interestingly, based on the data gathered, the most popular topic of choice for cybercriminals were spyware related searches, followed by entertainment news, with hosting sites, P2P and proxies related searches showing a significant growth. What's worth highlighting while interpreting the data, is that it's only valid for a specific period of time. How come? Controversial to the common misunderstanding that cybercriminals are picky about popular search terms, what they

do is automatically syndicate the Web's buzz for their malicious purposes.

Poisoned search engine results have been an active tactic in the arsenal of the cybercriminal for several years. The practice, known as [blackhat SEO \(search engine optimization\)](#), is now the primary source for hijacked legitimate traffic, which in a combination with the automatic compromising of hundreds of thousands of legitimate sites, exposes end users to everything a cybercriminal has to offer.

Go through related posts:

[Cybercriminals syndicating Google Trends keywords to serve malware](#)
[Federal forms themed blackhat SEO campaign serving scareware](#)
[9/11 related keywords hijacked to serve scareware](#)
[Haiti earthquake themed blackhat SEO campaigns serving scareware](#)
[The ultimate guide to scareware protection](#)

Although, Google's aware of the situation, and is catching up pretty fast, cybercriminals remain ahead of the game, doing nothing else but playing by the SEO book. For instance, in a [report released by Google in April](#), the company found out that scareware accounted for 15% of all malware, and that scareware represented 50% of the [malware delivered through malvertising](#). The thing evasive practice that cybercriminals took advantage of to achieve these results, is by [checking for the correct HTTP referrer](#).

Poisoned search engines are the inevitable result of the real-time Web, allowing cybercriminals to take advantage of the same tools and tactics, that legitimate marketers do. But being the market leader in online search, means that in 2010 your crawlers shouldn't be that easily tricked into loading the legitimate content, with the malicious one served to the average Internet user.

What do you think? Is Google doing enough to protect its users from poisoned search engine results? Most importantly, can Google [protect the end user from himself](#) at the end of the day? Would the current situation have been any different if, for instance, Bing or Yahoo was the market share leader in online search?

Talkback.

Google tops comparative review of malicious search results -- again | ZDNet

Using which search engine has the highest probability of landing you on a malicious web site? According to a [newly released report by Barracuda Labs](#), that's Google -- [again](#) .

The methodology of the study was fairly simple. The researchers set up a system which would automatically search using trending keywords in order to find out which search engine, Google, Yahoo Search!, Bing or Twitter would serve a malicious result. The findings:

In June, Google was crowned “King” of malware, containing 69% of the malware. By December, that number decreased by 45% to Google containing 38% of the overall malware. This shows that attackers have not only increased the amount of overall search engine malware but also have decided that it is worth targeting other search engines besides Google.

34,627 malware samples found
1 in 1000 search results lead to malware
1 in 5 search topics lead to malware
Number 2 Search Term Leading to Malware: “Jenni J-Woww”

Although compared to the previous study, Google's market share is diminishing, the number is still high taking into consideration the fact that Google remains the most widely used search engine [followed by Bing](#).

Meanwhile, cybercriminals are no longer interested in building diverse content farms, as much as they are interested in exploiting the real-time nature of the Web, by automatically hijacking keywords from Google Trends and Yahoo Buzz. They follow the trends, hence the increase in malicious results on Bing.

Search engines and blackhat SEO (search engine optimization) attacks continue representing a prominent tactic in the arsenal of the malicious attacker.

See also:

[Google tops comparative review of malicious search results](#) [The Web's most dangerous keywords to search for](#) [Cybercriminals syndicating Google Trends keywords to serve malware](#) [The ultimate guide to scareware protection](#) [Google: Scareware accounts for 15 percent of all malware](#)

Google to introduce warnings for potentially hackable sites | ZDNet

Last week, Google's Patrick Chapman and Matt Cutts announced that [they're experimenting with a new security feature](#) aiming to alert webmasters on the potential for having their sites hacked due to the outdated version of their web applications, starting with Wordpress only :

"Recently we've seen more websites get hacked because of various security holes. In order to help webmasters with this issue, we plan to run a test that will alert some webmasters if their content management system (CMS) or publishing platform looks like it might have a security hole or be hackable. This is a test, so we're starting out by alerting five to six thousand webmasters. We will be leaving messages for owners of potentially vulnerable sites in the Google Message Center that we provide as a free service as part of Webmaster Tools.

One of the most popular pieces of software on the web is WordPress, so we're starting our test with a specific version (2.1.1) that is known to be vulnerable to exploits. If the test goes well, we may expand these messages to include other types of software on the web."

Whereas the upcoming feature is a great proactive measure, [WordPress isn't necessarily the blogging platform of choice](#) for the majority of cybercriminals and blackhat search engine optimizers looking for efficient ways to acquire traffic. In fact, the current tools and tactics that they take advantage of, attempt to inject their presents onto each and every known to be remotely exploitable web application. This automated approach often building hit lists through [search engines reconnaissance](#) , is many steps ahead of Google's anticipated feature, so if they truly want to [slow down the automated reconnaissance process](#) , they could easily start challenging these automated crawlers.

Web application specific attacks are happening, but the applications or blogging platforms' susceptibility to exploitation as a key success factor was replaced by a "target everyone, everywhere" model, and the results in terms of the hundreds of thousands of sites remaining affected are pretty evident. Today's threatscape not only [empowers lone cybercriminals](#) with the tools necessary to inject malware and redirection scripts on hundreds of thousands of vulnerable sites automatically, but has long reached the stage when publicly released exploits for remotely exploitable web applications are automatically syndicated for real-time hitlist building.

In May, [Google introduced the Safe Browsing diagnostic](#) as a reactive response to the increasing number of web sites hosting or redirecting to malware, so the key to providing value to webmasters using the new warnings feature, would be to diversify the list of vulnerable web applications, and perhaps most importantly - emphasize and point out to related tools and services aiming to allow webmasters to self-audit their web sites.

Google: Spam volume for Q1 back to pre-McColo levels | ZDNet

It took only a couple of months for cybercriminals to catch-up and reintroduce the massive spam volumes that briefly disappeared following the [shutdown of the cybercrime ecosystem's sitting duck McColo](#) in November, 2008.

According to [Google's Postini Spam data and trends for Q1 2009](#) , during the first quarter of the year the spam volume was the strongest since 2008, increasing with an average of 1.2% per day. Data from [Cisco's IronPort](#) and [Symantec's MessageLabs](#) confirms the trend.

Spammers have recovered from the McColo shutdown - it's a fact. But with Conficker in a standby mode, it's worth discussing the (mini) botnets currently responsible for the increasing spam volume, and how have spammers adapted in order to improve their resilience to potential attempts to shut down their operations.

According to Marshal's TRACE team, the [resurrection of the Rustock botnet](#) accounted for 35% of all the spam they were monitoring in March, with the Mega-D botnet once again topping [the chart of spambots](#) . And even though these are the "usual suspects" that migrated to alternative [cybercrime-friendly ISPs](#) , partitioned botnets usually [remain beneath the radar](#) , to form the foundation for the growing use of [managed spam services](#) consisting of a relatively small number of infected hosts.

Spammers are also game changers. For instance, on their way to exploit the trust hierarchy among legitimate email service providers -- think DomainKeys -- vendors of spamming services have looking for ways to become [DomainKeys verified spammers](#) since early 2008. With two frameworks currently offered as a managed service, sooner or later spammers will be able to start taking advantage of spam platforms on the basis of legitimate infrastructure. With the [efficient abuse of CAPTCHA authentication](#) thanks to outsourcing the process, hundreds of thousands of bogus email accounts at

legitimate email service providers are being automatically abused for the purposely of sending spam ([Spam coming from free email providers increasing](#) ; [Gmail, Yahoo and Hotmail systematically abused by spammers](#)).

With decentralization of command and control locations/communications, and standartization of the spamming process with quality assurance in mind in the face of managed spam services, spam, in between the rest of the malicious activities streaming from the infected hosts, are not going away. Interestingly, despite the fact that the money made from spam look like pocket change compared to the money made from rogue security software and the process of monetizing the botnet by partitioning it ([Into the Srizbi's botnet business model](#) ; [Money Mule Recruiters use ASProx's Fast Fluxing Services](#)) cybercriminals won't given up on their [equally distributed revenue stream](#) .

Google: Scareware accounts for 15 percent of all malware | ZDNet

In an upcoming research entitled ["The Nocebo Effect on the Web: An Analysis of Fake AV distribution"](#), Google's Security Team is about to release the results from their 13 month study into the growth of fake security software, also known as scareware or Fake AV.

[A preview of their findings](#):

The analysis is based on 240 million web pages used as a sample 11,000 domains involved in Fake AV distribution discovered based on the sample

Fake AV currently accounts for 15% of all malware Google detects on the web

Fake AV attacks account for 60% of the malware discovered on domains that include trending keywords

Fake AV is responsible for 50% of all malware delivered via Ads

What's the first thing that makes an impression based on these findings? It's the small number of domains they were able to identify, despite the fact that 60% of the domains hijacking trending topics serve scareware, and that 50% of all malware delivered through malvertising is fake AV.

Go through related posts: [The ultimate guide to scareware protection](#) ; [FBI: Scareware distributors stole \\$150M](#)

This number is the effect of the active evasive practices applied in order to trick Google's crawlers, by serving them legitimate content, and the malicious one to the unaware end user.

Cybercriminals have been abusing Google Trends ([Cybercriminals syndicating Google Trends keywords to serve malware](#) ; [Syndicating Google Trends Keywords for Blackhat SEO](#)) for scareware or malware serving purposes for years.

The same, although in smaller proportions, has been taking place through legitimate ad networks ([Malware-infected WinRAR](#)

[distributed through Google AdWords](#) ; [Scareware Campaign Using Google Sponsored Links](#)), with malvertising (the practice of [serving malicious content through legitimate ad networks](#)) already trending.

How are cybercriminals tricking Google's crawlers in the first place? In the very same way search engine optimization scammers have been doing since the early days of the Web - through [content cloaking](#) , through Google's playbook by using *noindex*, *nofollow*, *noarchive* tags, and through one of the most effective practices used by blackhat SEO campaigners these days - the http referrer:

```
"var ref,i,is_se=0; var se = new Array("google. ","msn. ","yahoo. ","comcast. ","aol. "); if(document.referrer)ref=document.referrer; else ref=""; for(i=0;i<5;i++)"
```

Since a crawler isn't using http referrers, and isn't browsing the web using a user agent ([How the Koobface Gang Monetizes Mac OS X Traffic](#) ; [Mac OS X user agent check](#)) that the cybercriminal would like to serve malicious content to, they are easily capable of covering up their tracks, sometimes even from the eyes of the security researcher who's trying to profile their campaigns starting from somewhere in the middle of the URL redirection chain.

Pragmatic tips for preventing scareware infections:

Go through [ZDNet's Guide to Scareware Protection](#) , explaining the basics of what scareware is, the tactics used by the cybercriminals to spread it, as well as the main characteristics of the scam. Even better, share the link to the guide with your social circle in an attempt to raise awareness on one of the most prolific monetization tactic cybecriminals use these days.

In 99% cases of the scareware infection attempts, the user is in control of situation. The remaining 1% are the campaigns where [scareware is pushed through client-side exploits](#) , or through a [botnet the user is unknowingly participating](#) in. Since scareware is relying entirely on the use of social engineering and legitimately looking "You're Infected!" pop-ups, learning the characteristics of the scam would help you to spot and avoid executing the binary it's enticing you to do.

Although perceived as a prank by some, [scareware has been](#)

[converging with ransomware](#) for a while now. Realizing the mess that could take place with a scareware variant locking down your PC, or encrypting key files on it, is logically supposed to increase the end user's vigilance in those cases where their Internet Security Suite doesn't alert them in the first place.

Don't bother attempting to verify the legitimacy of *Mega Antivirus Solution 2010* , since cybercriminals systematically rebrand the same piece of scareware with a different name. In fact, a common practice these days is to see scareware A using a blackhat SEO campaign by promising to remove scareware B. Use a basic **tcp wrapper hosts.deny: ALL** approach - automatically assume the worst, and basically [check whether the software](#) pretending to be [legitimate is actually real](#) .

Browsing the Web in a [sandboxed environment](#) , using [least privilege accounts](#) , and ensuring you are [free of client-side exploitable flaws](#) will mitigate a huge percentage of the risk.

Google is set to release their complete report at the end of the month. The company is the best position to make an impact in the fight against scareware through the [SafeBrowsing project](#) , now an inseparable part of modern browsers. An update will be posted as soon as the research becomes public.

Google: no evidence of a Gmail vulnerability

| ZDNet

Following the [speculations on the resurrection](#) of what's thought to be an [already fixed Gmail flaw](#) which could assist in [domain name hijackings](#) , yesterday [Google commented](#) that their investigation indicated that the recent domain hijacks should be attributed to a phishing campaign, rather than to a Gmail flaw. The phishers was silently adding filter rules to the compromised Gmail accounts, then resetting the passwords so that the accounting data for a particular service or a domain would be quietly forwarded to the attacker's mailboxes.

"With help from affected users, we determined that the cause was a phishing scheme, a common method used by malicious actors to trick people into sharing their sensitive information. Attackers sent customized e-mails encouraging web domain owners to visit fraudulent websites such as "google-hosts.com" that they set up purely to harvest usernames and passwords. These fake sites had no affiliation with Google, and the ones we've seen are now offline. Once attackers gained the user credentials, they were free to modify the affected accounts as they desired. In this case, the attacker set up mail filters specifically designed to forward messages from web domain providers."

Phishing campaigns impersonating Google are in fact becoming so prevalent, that an entire market segment within the underground economy is starting to emerge, which is primarily trading with stolen AdSense accounts. Access to these accounts is obtained either through data mining already infected with malware hosts part of their botnet, or through plain simple [phishing campaigns taking advantage of typosquatting](#) in order to visually social engineer an end user, consider the following examples :

| | |
|---------------------------------------|----------------|
| adwords.google.com.index.main.update | .qwertycn.cn |
| adsense.google.com.server.main.update | .dirty-boy.cn |
| edit.google.com.main.update | .the-format.cn |
| google.com.urchin.js | |

.7traff.cn google.com.urchin.js .axa1.cn adwords.google-
secutiyserv .com
google.com.br.updatesoftware.index.d81f0f02cd6a877358cde8fbdba
d89a5 .qwertycn.cn
google.com.updatesoftware.index.d81f0f02cd6a877358cde8fbdbad8
9a5 .rootit2.info adwords.google.com.session-
69680268279998252722.92444537268559875865 .com68.ru

Two weeks ago, Google quietly [fixed a critical XSS vulnerability](#) affecting its accounts login page, which at the time was providing a fully realistic opportunity for malicious attackers to turn into "cookie monsters" and hijack user's sessions on a large scale.

Google, Mozilla and Microsoft ban the DigiNotar Certificate Authority in their browsers | ZDNet

With the [DigiNotar saga](#) continuing, it's time to summarize some of the current events surrounding it.

According to multiple blog posts, [Google](#), [Mozilla](#) and [Microsoft](#) have already banned the DigiNotar Certificate Authority in their browsers. This preemptive move comes as a direct response to the mess that DigiNotar created by issuing over 200 rogue certificates for legitimate web sites and services -- see [a complete list of the affected sites and services](#).

Earlier this week, Google reported of [attempted man-in-the-middle attacks](#) executed against Google users, and most recently, TrendMicro offered insights into [a large scale spying operation launched against Iranian web users](#).

According to TrendMicro:

From analysis of Smart Protection Network data, we see that a significant part of Internet users who loaded the SSL certificate verification URL of Diginotar were from Iran on August 28, 2011. On August 30, 2011 most traffic from Iran disappeared and on September 2, 2011 about all of the Iranian traffic was gone and Diginotar received mostly Dutch Internet users, as expected.

These aggregated statistics from Trend Micro Smart Protection Network clearly indicates that Iranian Internet users were exposed to a large scale man-in-the-middle attack, where SSL encrypted traffic can be decrypted by a third party. For example: a third party probably was able to read all e-mail communication an Iranian Internet user has sent with his Gmail account.

Meanwhile, the [Dutch government issued a statement](#) saying that it "cannot guarantee the security of its own websites" and is "taking over the company's (DigiNotar) operations."

"the user of government sites no longer has the guarantee ... that he is on the site where he wanted to be," Interior Minister Piet Hein Donner said at a pre-dawn press conference.

Moreover, Illinois-based VASCO, which owns the Dutch-based DigiNotar [issued the following statement](#):

DigiNotar detected an intrusion into its Certificate Authority (CA) infrastructure, which resulted in the fraudulent issuance of public key certificate requests for a number of domains, including Google.com. Once it detected the intrusion, DigiNotar has acted in accordance with all relevant rules and procedures. At that time, an external security audit concluded that all fraudulently issued certificates were revoked. Recently, it was discovered that at least one fraudulent certificate had not been revoked at the time. After being notified by Dutch government organization Govcert, DigiNotar took immediate action and revoked the fraudulent certificate.

Who's behind the attacks? According to the [Tor Project](#), clues were found in one of the certificates, including messages in Farsi:

Of particular note is this certificate:CN=*.RamzShekaneBozorg.com,SN=PK000229200006593,OU=Sare Toro Ham Mishkanam,L=Tehran,O=Hameye Ramzaro Mishkanam,C=IR

The text here appears to be an entry like any other but it is infact a calling card from a Farsi speaker. RamzShekaneBozorg.com is not a valid domain as of this writing. Thanks to an anonymous Farsi speaker, I now understand that the above certificate is actually a comment to anyone who bothers to read between the lines: "RamzShekaneBozorg" is **"great cracker"**, "Hameyeh Ramzaro Mishkanam" translates to **"I will crack all encryption"**, "Sare Toro Ham Mishkanam" translates to **"i hate/break your head"**

VASCO, the owner of DigiNotar said it plans to [indefinitely suspend the sale of its traditional and extended-validation \(EV\) SSL certificates](#), until the case is solved. *"The company will only restart its SSL and EV SSL certificate activities after thorough additional security audits by third-party organizations"*.

Google intros advanced sign-in feature | ZDNet

The search engine giant has [introduced advanced sign-in feature](#) for its users.

The feature basically offers DIY two factor authentication, with users having to not only enter their passwords, but also, the code that they receive on their mobile devices, or generate for themselves.

Moreover, next to the code, the user is also presented with the opportunity to enter a backup phone number in case he loses access to the primary device.

Once you enable 2-step verification, you'll see an extra page that prompts you for a code when you sign in to your account. After entering your password, Google will call you with the code, send you an SMS message or give you the choice to generate the code for yourself using a mobile application on your Android, BlackBerry or iPhone device. The choice is up to you. When you enter this code after correctly submitting your password we'll have a pretty good idea that the person signing in is actually you.

[Microsoft's Hotmail offers a similar service](#) , with Yahoo! Mail currently in catch up mode.

See also:

[Hotmail's new security features vs Gmail's old security features](#)
[Google, Facebook: End Passwords, Get Biometrics. Now!](#)

Google introducing Safe Browsing diagnostic to help owners of compromised sites | ZDNet

Last week, Google's Niels Provos made an announcement regarding a newly introduced feature aiming to help owners of

compromised sites in understanding the implications of the compromise, as well as the malicious events that took place when Google last indexed the site. From [Google's Online Security Blog](#) :

We've been protecting Google users from malicious web pages since 2006 by showing warning labels in Google's search results and by publishing the data via the Safe Browsing API to client programs such as Firefox and Google Desktop Search. To create our data, we've built a large-scale infrastructure to automatically determine if web pages pose a risk to users. This system has proven to be highly accurate, but we've noted that it can sometimes be difficult for webmasters and users to verify our results, as attackers often use sophisticated obfuscation techniques or inject malicious payloads only under certain conditions. With that in mind, we've developed a Safe Browsing diagnostic page that will provide detailed information about our automatic investigations and findings.

These are some of the key benefits that I've already found highly effective in my investigative assessments.

despite that the data is kept for 90 days only, even a three months period of time with a snapshot of the malicious activity that's been going on at a particular domain is handy when conducting assessments, especially in those cases where the compromise has already been detected by the site owner, and the malicious links/scripts removed

the feature's investigative and relationship establishing nature in the sense of listing other sites compromised by the same malicious domain, as well as the domains where the malware was hosted acting as redirection points in this case, easily allow you to see the big picture from different angles regarding a particular malware

group or an incident

the endless possibilities for automation and integration of the data thanks to the Safe Browsing API, as well as the possibility to use the service as a early warning system for security incidents

What type of data is stored about a compromised site anyway? Google's Diagnostics answers four questions regarding a compromised site :

What is the current listing status for [the site in question]? What happened when Google visited this site? Has this site acted as an intermediary resulting in further distribution of malware? Has this site hosted malware?

Let's test the service and [diagnose Redmond Magazine](#) , which was among the high profile [victims of a recent SQL injection attack](#) , in order to demonstrate the type of data Google gathers. According to the historical situation at this domain :

Of the 59 pages we tested on the site over the past 90 days, 3 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 05/19/2008, and the last time suspicious content was found on this site was on 05/10/2008. Malicious software includes 3 trojan(s), 3 exploit(s). Successful infection resulted in an average of 5 new processes on the target machine. Malicious software is hosted on 2 domain(s), including ririwow.cn, jueduizuan.com. 2 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, including wowyeye.cn, ririwow.cn.

You can safely [test the service](#) by looking up the [fast-flux domain](#) which I mentioned in a previous post, or if curiosity prevails, diagnose the malicious domains injected in the [ongoing SQL injection attacks](#) .

The introduction of the Safe Browsing diagnostic feature is a step in the right direction - limiting speculations and empowering both, researchers, and the average end users with evidential data regarding a particular compromise. However, there have been and continue to be numerous successful attempts by malicious parties to trick Google's crawlers into flagging a malicious sites as a clean one. In fact, a huge number of the sites used as redirectors to malicious

domains in the recent SQL injection attacks, remained undetected, yet another indication that the bad guys change their tactics and adapt rapidly, sometimes more rapidly than we'd like to imagine they do.

Google introduces Safe Browsing Alerts for network administrators | ZDNet

On Thursday, the search giant [announced the availability of a new service](#) Safe Browsing Alerts for Network Administrators.

Basically, the service allows network administrators to monitor the networks they manage for malicious content. And best of all - the service is free. Originally [announced by Google last year](#), the service is apparently ready for prime time.

Network administrators can claim their AS ([Autonomous System](#)) [here](#).

Google fixes critical XSS vulnerability | ZDNet

All your accounting data are not belong to us. Hours after [a proof of concept](#) example detailing [a XSS vulnerability at Google's account login page](#) was posted at the XSS Project's clearing house, the company quickly took notice and fixed it.

"Security researcher "[Xylitol](#) " is credited with the discovery of this critical bug. In this case, the fact that SSL is being used on the login page, does not necessarily mean that the users' login information is secured. Malicious people can exploit this Google XSS to propagate malware, spyware, adware and steal authentication credentials."

In October, Google was criticized for not paying attention to an already reported cross domain frame injection vulnerability, prompting the release of [a proof of concept example](#) demonstrating how third-party content can be injected within Google pages. Ignoring [the endless debate of the pros and cons](#) of full disclosure, responsible disclosure and partial disclosure for a moment, the fact that a large number of already [reported vulnerabilities remain unfixed](#) despite the potential for abuse, clearly indicates a company's commitment -- or the lack of.

XSSed is a great open source resource, whose [early warning feature](#) and [RSS feeds](#) are an invaluable resource that could help the affected sites into prioritizing the fixing of particular flaw that's now in the public domain, if only were the affected companies to embrace it as such.

Google downplays severity of Gmail CSRF flaw | ZDNet

Yesterday, Vicente Aguilera Diaz from [Internet Security Auditors](#) released [proof of concept of a CSRF \(Cross-Site Request Forgery\) vulnerability in Google's Gmail](#) , which he originally communicated to Google two years ago. The CSRF flaw affects Gmail's "Change Password" function, since according to Diaz the session cookie is automatically sent by the browser in every request making the attack possible.

Google's response came fast, and it's in the form of - "[We do not consider this case to be a significant vulnerability.](#) " :

We've been aware of this report for some time, and we do not consider this case to be a significant vulnerability, since a successful exploit would require correctly guessing a user's password within the period that the user is visiting a potential attacker's site," the spokesperson said. "Despite the very low chance of guessing a password in this way, we will explore ways to further mitigate the issue. We always encourage users to choose strong passwords, and we have an indicator to help them do this.

Compared to the futile password guessing attempts in order to execute the attack, nothing can replace flaw-independent approaches like social engineering. From a pragmatic perspective, malicious attackers have an extensive number of tactics to choose from if they were trying to obtain your Gmail password. Starting from plain simple [phishing campaigns](#) , and going to a more [efficiency-centered](#) approaches - remember the [G-Archiver](#) fiasco?

Related posts: [Google downplays Chrome's carpet-bombing flaw](#) ; [Google: no evidence of a Gmail vulnerability](#) ; [Google fixes critical XSS vulnerability](#).

Google's most recently fixed flaws across its web properties include October 2008's [cross domain frame injection vulnerability](#) , November 2008's [XSS in Google's accounts SSL login page](#) , and January 2009's [Google sites reflective cross-site scripting flaw](#) .

Google downplays Chrome's carpet-bombing flaw | ZDNet

In a recent [Q&A with Google's Brian Rakowski](#) , Philipp Lenssen asked him a question in regard to Chrome's [carpet-bombing flaw](#) . Not surprising, considering that [Apple refused to admit Safari's carpet-bombing flaw](#) at the first place, Google is too, downplaying it :

"Lenssen : There are ways to make Chrome automatically download a file without the user confirming this (at least using Chrome's default options). Don't you consider that a potential problem?

Rakowski : On its own, downloading a file isn't dangerous. It can be annoying if a site tries to download a bunch of files to fill up your hard drive, but there are other ways to do things like that and it hasn't become a problem. The danger arises when an automatically downloaded file can be automatically executed. We've taken steps to prevent this in Google Chrome and will continue to make sure that this is the case. "

In reality, the danger arises from an **automatically downloaded malicious file** with a changed icon and a descriptive title or [backdoored but legitimate Windows Office files](#) downloaded without any notice, not from dumping hundreds of files on a particular desktop. Causing a denial of service attack next to dumping a piece of crimeware isn't really going to do much for a malicious attacker wanting your Ebanking data.

The level or [exploitability of any of Chrome's vulnerabilities](#) is proportional with its market share, and whereas there are no

currently active malware attacks taking advantage of this particular flaw allowing them to dump a file on a visitor's desktop, leaving this opportunity open won't go unnoticed. As it appears, coming up with a simple script filling up someone's hard drive upon visiting a specific site, seems to be the way to raise awareness on the potential for old school malware attacks relying on changed icons and the binaries

spread across the desktop, and hopefully attract Google's attention to the possibilities for abuse.

Chrome's been receiving lots of criticism internationally, with [Germany's Federal Office for Information Security](#) urging users not to use the browser, next to the Dutch Computer Emergency Response Team (Govcert.nl) recommending its use [only in test environments](#) due to the BETA release. For the time being, it's clearly a wait and see how they threat security issues type of situation.

Google-China cyber espionage saga - FAQ | ZDNet

With more details emerging on the inner workings of the targeted malware attack that hit Google and over 30 other companies ([ZDNet News Special Coverage - Special Report: Google, China showdown](#)), it's time to summarize all the events that took place during the past week, and answer some of the most frequently asked questions such as - How did the attack take place? Did Google strike back at the attackers? Was the Chinese government behind the attacks, and if not who orchestrated them and for what reason?

Go through the FAQ and their answers.

Q: Which companies were affected in the targeted malware attacks?

According to the initial [post confirming the targeted malware attacks](#), Google stated that *"at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted."*

On the same day, actual details on who's been targeted started to emerge, prompted by Google's decision t

o go public with the incident at the first place, with Adobe being the first company to confirm the "[corporate network security issue](#)", later on denying the initial allegations that the attacks took place [through a zero day flaw in Adobe's Reader](#).

According to public reports, the number of affected companies increased to 34, including [Yahoo, Symantec, Northrop Grumman and Dow Chemical](#). Of those, only [Yahoo](#), [Juniper Networks](#) and [Symantec](#) provided details that they're currently investigation possible security incidents without actually confirming that their networks may have been successfully compromised in the attacks.

A day after Google's announcement of the incident, the law firm [Gipson, Hoffman and Pancione](#) which represents CYBERSitter in a

[\\$2.2 billion lawsuit](#) against China for pirating source code and using in Green Dam, a [content filtering](#) / [censorship program](#) , reported that "[it has suffered cyber attacks originating from China](#)".

Q: How did the attack take place?

Through a combination of [spear-phishing \(targeted attack\)](#) , and a zero day flaw ([CVE-2010-0249](#)) affecting [Microsoft's Internet Explorer](#) (see which versions and which platforms are affected).

[Microsoft is currently working on emergency patch](#) , given the fact that the exploit code used in the attack is now publicly available, with the governments of [Germany](#) and [France](#) urging users to [stop using Internet Explorer](#) .

Not only did the targeted malware attack managed to bypass the malware/spam filters of the organizations ([Phishing experiment sneaks through all anti-spam filters](#) ; [New study details the dynamics of successful phishing](#)), but also, managed to successfully exploit hosts within the working environment which allowed the attackers to [steal intellectual property from Google](#) .

Upon the successful exploitation of these hosts, the attackers relied on [the Hydraq trojan](#) in order to facilitate the theft of intellectual property ([Trojan.Hydraq Exposed](#) ; [Trojan.Hydraq - Part II](#)), and continue maintaining access to the affected hosts.

Q: Were the attacks indeed one of the "most sophisticated" ever seen as claimed by certain security vendors?

In order to say that something is ["most sophisticated"](#) , you'd first have to compare it with a related incident/piece of malware. The Google incident is often cited as "ultra sophisticated" due to the quality of the malware code, and the successful "segmentation of the attack population" or the practice of finding the names and emails of prospective victims to be targeted within a particular enterprise. However, no matter how sophisticated the code, [compared to Conficker](#) , this incident is basically a targeted malware attack exploiting a zero day flaw that ultimately drops a coded from scratch piece of malware.

Malware code sophistication shouldn't be a criteria for a state-sponsored operation due to the availability of ["malware coding for](#)

[hire](#)" services allowing potential customers to have [their own sophisticated piece of malware](#) , coded by the very same malware authors whose creations fuel the growth of today's crimeware epidemic.

Moreover, the concept of using zero days for targeted attacks is nothing new. Similar [targeted attack relying on MS Word zero day](#) against U.S Department of State computers took place in 2007. So are there are key differentiation factors left? It's the question how did they manage to obtain the emails used in the targeted attacks of so many companies. And with no company offering additional insights on the nature of the campaign structure used, for instance were the attackers relying on "event-based social engineering" tactic, we can only speculate on the ease or sophistication when tricking employees into clicking on the links.

There are numerous ways in which the attackers obtained the emails, including internal ones which are not publicly available. One of these practices is called [OSINT \(open source intelligence\) through botnets](#) , a concept that's been around since the first time botnets were perceived as a tool for conducting espionage. With the ability to geolocate the physical location or network location of the entire botnet, a botnet master can easily filter the availability of infected hosts within a particular company's netblock, country, even city, and from there can data mine and engage in hit list building for future targeted malware attacks.

In 2007, [Support Intelligence's "30 Days of Bots" experiment](#) successfully located malware -infected hosts within the networks of Fortune 1000 companies, with these compromises making it possible to collect internal emails, map the network structure etc.

[Next](#) -->

Q: What kind of information was stolen and accessed without authorization?

According to Google, which is the only company that has publicly acknowledge the security incident, the theft from their network was targeting intellectual property, as well as several Gmail accounts which according to the company belong to human rights activists in China. The rest of the affected companies, deny discussing such

security incidents possibly due to the negative publicity, and therefore do not confirm nor deny that intellectual property was stolen.

The claim that these accounts were accessed is perhaps the most notable connection with the Chinese government, considering the fact that the command and control servers were not located in China. And even if they were, it would basically mean that the Chinese Internet which is well known for its widespread abuse, and often maintains the top position for spam and malware sending, could have been abused by a third-country, or international enterprise engaging in espionage while risk forwarding the attacks to a known bad network.

[Why would a Chinese government spy hack Google in order to attempt reading the content of several Gmail accounts](#) , compared to taking the much more effective approach, one that they've been relying on so far, namely, individually attempting to infect human rights activists with malware, instead of taking the exotic approach of exposing themselves by compromising Google? In September, 2009, [Chinese hackers launched targeted attacks against foreign correspondents](#) , not by hacking their ISPs, but by targeting them individually part of the [GhostNet cyber espionage campaigns](#) .

Q: Where were the command and control servers located, and does it really matter at the bottom line?

In short, the physical location of the command and control servers doesn't really matter in the sense that for years, [malware infected hosts have been used as stepping stones \(island hopping\)](#) for increasing a cybercriminal's anonymity ([The Cost of Anonymizing a Cybercriminal's Internet Activities](#) ; [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two](#)), risk hedging of getting caught and risk forwarding the responsibility for a particular security incident to the country in question. This very same approach was utilized by the attackers, and is a daily routine for a huge percentage of cybercriminals.

They not only relied on "island hopping", but used U.S based command and control servers based in [Illinois, Texas, and several ones in Taiwan](#) . Managed hosting provider Rackspace quickly

responded to some of the claims by [confirming that one of their servers was compromised](#) and was indeed participating in the targeted malware attack.

What about the historical reputation of the command and control servers/IPs involved in the campaign. [According to VeriSign iDefense](#) - *"it has spoken to "two independent, anonymous sources in defense contracting and intelligence consulting." They told it the source IPs and drop server of the attack had been traced back to systems associated with agents of the Chinese state, or their proxies. "*

The following is a [complete list of the domains](#) involved in the [targeted malware attack](#) :

| | | |
|-------------------------|---------------------|---------------------|
| 360.homeunix.com | 69.164.192.4 | alt1.homelinux.com |
| amt1.homelinux.com | aop1.homelinux.com | app1.homelinux.com |
| blogspot.blogspot.org | filoups.info | ftp2.homeunix.com |
| ftpaccess.cc | google.homeunix.com | members.linode.com |
| sl1.homelinux.org | sl1.homelinux.org | tyuqwer.dyndns.org |
| update.ourhobby.com | | voanews.ath.cx |
| webswan.33iqst.com:4000 | yahoo.8866.org | ymail.ath.cx |
| yahooo.8866.org | sl1.homelinux.org | 360.homeunix.com |
| ftp2.homeunix.com | | update.ourhobby.com |
| connectproxy.3322.org | csport.2288.org | |

[Next](#) -->

Q: Did Google strike back at the attackers?

Apparently, [engineers at Google gained access to a computer in Taiwan](#) , and by doing so, saw evidence of the ongoing attacks targeting at least 33 other companies.

Q: What other actions is Google currently undertaking in response to the security incident?

Google is not only considering the option of leaving the Chinese Internet market citing human rights violation concerns and the recent cyber espionage attacks, but is also soliciting the support of major U.S technology companies. However, the rest of tech giants appear to be fully anticipating the business potential of China's market.

[Quoted on Bloomberg](#) , Chuck Mulloy, a spokesman for Intel, stated that they haven't seen evidence of a "broad-based attack". [Microsoft's Steve Ballmer was quoted as saying](#) that *"every large institution is being hacked"*, with [HP's Mark Hurd sharing a similar view](#) with the Financial Times quoted as saying *"I'd hate to run off on this one example and say it's a threat to the evolution of the IT industry"*.

Moreover, [Google has not only given its China employees a holiday leave](#) , but appears to be investigating possible insider participation in the attacks, with workers there no longer having access to their computers until the investigation is over.

Q: Did the targeted malware attack receive any political attention?

With Google's bargaining power, that was pretty obvious. On the same day that they announced the targeted malware attack, U.S Secretary of State Hillary Rodham Clinton, issued a "[Statement on Google Operations in China](#) "

"We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. I will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear."

More reactions followed from [Anna G. Eshoo's response to the attack on Google](#) :

"I'm deeply disturbed that yet another wave of attacks is coming from China. This raises serious national security concerns. I commend Google for coming forward with information about this attack and for cooperating with law enforcement officials to investigate the origin and nature it. It is important that companies continue to be transparent and open about cyberthreats.

"For far too long, cyberattackers have hidden in the shadows. These kind of attacks are unacceptable and undermine confidence in the global economy. I urge other companies possessing such

information to come forward to help the government identify the source of these attacks, so that the criminals can be held accountable for their actions."

And from [Loretta Sanchez's commentary](#) :

"This attack was a blatant, illicit attempt to access the private information of Google users who the government perceives to be a threat. If China turns out to be the perpetrator, it should be strongly condemned for its actions, which violate the internet's core principles of free speech and expression.

"At the same time, I applaud Google's decision to risk its lucrative Chinese contracts for the sake of these principles. In the past, Google and other internet providers have struggled to provide their Chinese users with a free and open forum in the face of government opposition. I sincerely hope Google's threat to sever its ties with China completely will compel not only the Chinese government but other regimes - like Vietnam - to finally expand free speech on the Web."

Q: What was the international community's response to the cyber espionage fiasco?

[Yahoo!'s China partner Alibaba Group](#) commented on Yahoo!'s alignment of positions with Google's:

"Alibaba Group has communicated to Yahoo! that Yahoo's statement that it is 'aligned' with the position Google took last week was reckless given the lack of facts in evidence," the firm's spokesman John Spelich told AFP in an email. Alibaba doesn't share this view."

Yesterday, [India's National Security Advisor M K Narayanan](#) , was quoted as saying that his office and other departments were also targeted with cyber attacks coming from China:

"Mr Narayanan told The Times that his office and other government departments were targeted on December 15 the same date that US companies reported cyber attacks from China. He said the attack was in the form of an e-mail with a PDF attachment containing a "Trojan" virus that allows hacker to access a computer remotely and download or delete files. After detecting the virus,

officials were asked not to log on until it was eliminated. "This was not the first instance of an attempt to hack into our computers," Mr Narayanan said."

Interestingly, in the past week everyone that ever experienced a security incident and believed that China was behind it, is deciding to go public with their claims. In particular [human rights activists blaming Chinese authorities for compromising their email accounts](#) .

Historically, there hasn't been a country that missed to blame China for the ongoing cyber attacks hitting their networks. [Germany in 2007](#) , the [U.K in 2007](#) , [France in 2007](#) , and [New Zealand again in 2007](#) all went public with allegations that China was responsible the cyber attacks hitting their networks.

Q: Did China issue an official response to the allegations?

[China's only official response](#) so far as been that "*China's internet is open and the Chinese government encourages development of the internet. Chinese law proscribes any form of hacking activity.* "

[Next](#) -->

Q: Was the Chinese government indeed behind the cyber espionage campaign?

There are a few key factors to consider before answering this question, and jumping to conclusions.

The first one is the difference between a government-sponsored and government-tolerated cyber attack. Government-sponsored cyber attacks are directly state funded hacking/cyber warfare activities aiming to achieve a specific government agenda, with the authorities themselves having control over the organizational and execution process. This type of cyber attacks are harder to prove due to the evasive practices the government in question could apply in order to avoid the potential scandal if detected.

But the very notion that Chinese authorities sponsored, endorsed, set the agenda for, and participated in the organization and execution process in regard to the Google incident is something I doubt they would get their hands dirty with at the first place. But how come? Even though that they can hedge the risk of getting caught, by forwarding the responsibility to third-party individuals unaware

who they're really working for, if a clear long-term agenda is given to their local hacktivist groups, they would successfully migrate from the incriminating government-sponsored attack to a government-tolerated one.

China, just like Russia has among the most vibrant hacktivist movements with skilled and self-mobilizing individuals that have proven no need from government interference in important hacktivist incidents such as [Georgia's DDoS attacks](#) , or the crowdsourcing attack on CNN courtesy of Chinese hacktivists ([The DDoS Attack Against CNN.com](#) ; [Chinese Hacktivists Waging People's Information Warfare Against CNN](#)). It's a people's information warfare using national dignity and overall collectivism within a society as the key incentive.

By allowing/tolerating their local hacktivist/hacking/cybercrime communities to flourish, the countries end up with an endless pool of human resources, from whose activities they can directly benefit, most of the time without the individuals themselves even aware of the practice, thinking it's their game. This strategic migration from a government-sponsored to a government-tolerated attack is what makes this question hard to answer with a definite yes, or a definite no, since it's all a matter of perspective.

Every country's private sector would love to have a government conducting corporate espionage for them and then passing on the obtained intellectual property. In this particular case, no country's cyber spies would expose themselves in a such way that the supposedly Chinese government sponsored Google hackers did. It's simple logic. Even more interestingly, so far I haven't come across a single opinion even considering for a second the possibility for a [private sector espionage operation](#) .

Both, a country's government and its private sector have the resources and the motivation to engage in such activities. And since the recent espionage campaigns were aiming to steal intellectual property from the private sector, it may well be another well funded private sector company engaging in unethical competitive advantage gaining practices by outsourcing.

Even though it's fairly logical to assume that China's government spies are truly interested in stealing intellectual property from military contractors, case in point is this [on-going targeted attack against US Military contractors](#) , by maintaining a government-tolerated cyber attacks policy, the China may in fact be collecting the fruits from the hacking activities on behalf of its vibrant and technically sophisticated hacktivist community.

Q: Has China ever complained of similar targeted malware attacks against its networks?

But of course. In [2008 China declined to comment the source of similar cyber espionage attacks](#) hitting their "core networks" but pointed out that 80% of the hosts involved were based in the United States.

Does this automatically mean that U.S based cyber warriors are behind the cyber espionage attempt? Not necessarily, since compromised hosts has been used as stepping stones ([island hopping](#)) can easily make it look like the compromised country's hosts actually belong to the physical attacker himself.

[Cyber espionage activities](#) courtesy of different nations continue making the headlines every on a regular basis. For instance, in 2008 [South Korean Army officers were hit with North Korean spyware](#) , and German spooks admitted [using a "trojan horse" to spy on Afghan politician and SPIEGEL journalist](#) again in 2008.

One thing remains certain, [even if Google leaves the Chinese Internet market](#) , it would still remain vulnerable to the very same threats that each and every enterprise connected to the Internet is facing these days. Moreover, the Google-China cyber espionage saga is not your typical black and white situation. And just like espionage in general, it's always a colorful case.

What do you think? Was the [cyber espionage incident sponsored by the Chinese government](#) or was it a private sector operation looking to steal intellectual property from major U.S tech companies? Does it really matter who was behind the attack, considering the fact that the networks of major companies got indeed compromised, and data stolen?

Do you believe that approaching China on this incident would have any significant impact rather than "we're investigation" response, or what other long-term actions should be taken in general? Perhaps emphasize on the [actual incident and its impact on business continuity](#) , instead on trying to figure out who did taking into consideration the fact that they won't stop doing it?

TalkBack.

Google and T-Mobile push patch for Android security flaw | ZDNet

During the weekend, Google and T-Mobile [pushed a patch](#) fixing [last week's disclosed security flaw affecting Google's Android](#) . The [flaw and the PoC](#) were communicated to Google on October 20th, with the vulnerability itself made possible due to Android's use of outdated third-party software packages.

"Users of the G1 Android phone on Friday have begun receiving a software update that fixes a flaw that security researchers found earlier in the week. The update included the fix to the browser vulnerability and a couple of other minor changes as well, said Michael Kirkland, a Google spokesman. Every user of the G1 may not have gotten the update yet but should within a short time frame, he said. Google worked with T-Mobile USA, the only operator selling the device, to push the update out to users. The G1 went on sale last week, and T-Mobile has not disclosed how many have sold so far."

The same issue occurred back in March, when [multiple vulnerabilities were reported in Google's Android SDK](#) , the exploitation of which was once again made possible due to the use of outdated open source image processing libraries. If there's a pure Android security flaw that you're looking for, try the outdated software packages running on it for starters -- pretty similar situation to Microsoft's recent emphasis on how the exploitation of [third-party applications undermines their security](#) .

GoDaddy hit by a DDoS attack | ZDNet

Domain name registrar and web hosting provider **GoDaddy.com** , was [hit by a DDoS attack on Wednesday](#) affecting thousands of its shared hosting customers for several hours. GoDaddy's Communications Manager **Nick Fuller** confirmed the attack originally speculated to be an "outage", and responded to several questions about it.

Q: Was Wednesday's GoDaddy.com "outage" an actual DDoS attack, and if so, how severe was it?

A: Wednesday, Go Daddy experienced a mutating type of DDOS attack.

Q: Could you provide us with more details on the DDoS attack itself, was it aimed at disrupting GoDaddy's entire infrastructure (email, DNS servers) or was it basically attacking GoDaddy.com's webserver?

A: This attack was aimed at hosting servers.

Q: For how long was GoDaddy.com unreachable on Wednesday, and could you provide us with a rough estimate on the number of affected sites?

A: There was an intermittent service disruption to a small percentage of our hosting customers over a period of hours.

Q: This isn't the first time that GoDaddy's been hit with a DDoS attack. Do you attribute this pattern to GoDaddy's popularity in the sense that unethical competition might be behind the attacks, or perhaps you have a different perspective on who and why attacked the company?

A: It's our policy not to elaborate on any cyber attack. As you can appreciate, we don't want to give attackers any information that could benefit them.

Go through recent DDoS attack incidents - [AlertPay hit by a large scale DDoS attack](#) ; [BBC hit by a DDoS attack](#) ; [Anti fraud site hit by a DDoS attack](#) ; [Norwegian BitTorrent tracker under DDoS attack](#) ;

This isn't the first time that GoDaddy is getting DDoS-ed. Similar attacks took place in [2005](#) , and then again in [2007](#) .

Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers | ZDNet

Breaking Gmail, Yahoo and Hotmail's CAPTCHAs, has been an urban legend for over two years now, with [do-it-yourself CAPTCHA breaking services](#), and [proprietary underground tools](#) assisting spammers, phishers and malware authors into registering hundreds of thousands of bogus accounts for spamming and fraudulent purposes.

This post intends to make this official, by covering an underground service offering thousands of already registered Gmail, Yahoo and Hotmail accounts for sale, with new ones registered every second clearly indicating the success rate of their CAPTCHA breaking capabilities at these services.

Monitoring the service for over a month now, revealed that during the period its "inventory of automatically registered email accounts" was emptying itself, then restoring to its current position - in the thousands, with 1 to 2 new accounts registered per second. Moreover, it's important to point out that compared to situations where scammers are scamming the scammers, these people "deliver the goods" that they promise. Last week, they've also started offering Hotmail and Yahoo email accounts, again in the thousands. For the time being, there are 134, 670 Gmail accounts available for purchase, as well as 42,893 Hotmail, and 10,847 Yahoo email accounts. There's naturally a price discrimination applied, for instance, if you're buying up to 10k Gmail accounts, the price for 1k would be \$6, from 10k to 100k the price drops to \$5 for 1k, and if you're going to buy over 100k accounts, the price would be \$4 for 1k.

Considering the fact that researchers are already managing to achieve a recognition rate of of nearly 90% of Gmail's CAPTCHA, 58% for Yahoo's CAPTCHA, and over 92 for [Microsoft's CAPTCHAs](#), the incentives for malicious parties to start efficiently breaking it and build a business model on the top of this seem to have prevailed. Here's a paper courtesy of Microsoft's research team, outlining some

of the findings regarding [the insecurities of these CAPTCHA's in general](#) :

"The Google HIP is unique in that it uses only image warp as a means of distorting the characters. Similar to the

MSN/Passport and Yahoo version 2 HIPs, it is also two color. The HIP characters are arranged closed to one another (they often touch) and follow a curved baseline. The following very simple attack was used to segment Google HIPs: Convert to grayscale, up-sample, threshold and separate connected components.

This very simple attack gives an end-to-end success rate of 10.2% for segmentation the recognition rate was 89.3%, giving $(0.102)^* (0.893)^{6.5} = 4.89\%$ total probability of breaking a HIP. Average Google HIP solution length is 6.5 characters. This can be significantly improved upon by judicious use of dilate-erode attack. A direct application doesn't do as well as it did on the ticketmaster and yahoo HIPs (because of the shear and warp of the baseline of the word). More successful and complicated attacks might estimate and counter the shear and warp of the baseline to achieve better success rates."

Abusing the clean IP reputation of these reputable email providers, results in the flood of spam coming from legitimate domains, as well as the easy of registering [bogus Blogspot accounts known as splogs](#) , for blackhat search engine optimization, [even malware, with Storm Worm](#) diversifying its propagation vector to using Blogspot accounts presumably buying the already registered accounts.

With the continuing supply of bogus email accounts efficiently registered by breaking the CAPTCHAs at these services, isn't it time for major web companies to start considering [replacements for text based CAPTCHAs like these ones](#) , or perhaps put more efforts into slowing down the currently [efficient text based recognition of their CAPTCHAs](#) ?

Gmail, Yahoo and Hotmail systematically abused by spammers | ZDNet

With the industry's eyes [constantly](#) monitoring [the usual suspects'](#) use of [phony hosting providers](#) , another market segment within the underground marketplace has been developing beneath the radar, aiming to build a malicious infrastructure ([Spammers targeting Bebo, generate thousands of bogus accounts](#) ; [Malware and spam attacks exploiting Picasa and ImageShack](#)) through efficient CAPTCHA recognition.

The latest [MessageLabs Intelligence annual report](#) for 2008 indicates that on average, 12 percent of the spam volume that they were monitoring in 2008 came from legitimate email providers such as Gmail, Yahoo Mail and Hotmail, followed by its September's peak of 25%. Earlier this year, more vendors emphasized [on this ongoing development](#) , citing machine learning CAPTCHA breaking techniques as the cause of it. In reality though, the very same humans that CAPTCHA was meant to identify continue undermining it as an anti-bot registration measure.

Researching the market segment throughout the year ([Microsoft's CAPTCHA successfully broken](#) ; [Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers](#) ; [Spam coming from free email providers increasing](#) ; [Spammers attacking Microsoft's CAPTCHA -- again](#) ; [Inside India's CAPTCHA solving economy](#)) it's time to assess the current situation and speculate on the upcoming efficiency model.

"In 2008, spammers developed an affinity for spamming from large, reputable web-based email and application services by defeating CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) techniques to generate massive numbers of personal accounts from these services. In January, 6.5 percent of spam originated from these hosted webmail accounts, peaking in September when 25 percent of spam originated from

these sources, averaging about 12 percent for the remainder of the year."

Three of the most popular free email providers continue being systematically abused by cybercriminals so efficiently, that they often top the charts ([Gmail](#) ; [Yahoo](#) ; [Microsoft](#)) of major anti-spam organizations such as [Spamhaus](#) . Despite that the affected companies are aware of this ongoing abuse, some of their mail servers have such [a bad reputation](#) due to the outgoing spam that it would be hard not to assume that sent email may not be reaching its destination. Moreover, [BorderWare's ReputationAuthority.org](#) also comes handy when assessing the reputation of [Gmail](#) , [Yahoo Mail](#) and [Hotmail](#) . Who's got the worst reputation varies, but for the time being, Microsoft's web properties appear to be ahead of Gmail and Yahoo's.

Is the supply of pre-registered accounts at these services driving the market, or is the customer's demand that's actually driving it? Whatever the case, supply is pretty efficient for the time being. For instance, I'm currently monitoring several web based bogus account registration services, with an average price for a thousand accounts at any of these email providers of \$10. That's right, for \$10 a spammer could get his hands on a thousand pre-registered email accounts if we are to exclude the discounts offered for a bulk purchase. And whereas I still haven't been able to establish a relationship between these services and [Indian CAPTCHA breakers](#) , theoretically, the supply of bogus accounts offered by a Russian service could be in fact outsourced as registration process to human CAPTCHA breakers, and the service itself acting as an intermediary. Whether it's the use of malware infected hosts, or through human CAPTCHA solvers, the hundreds of thousands of accounts offered for sale remain there.

Let's talk about efficiency. A research paper entitled "[Exploiting the Trust Hierarchy among Email Systems](#) " released earlier this year, and surprisingly receiving zero media attention, shows a proof of concept allowing the researchers to not only bypass Gmail's messages limit for bulk messages, but also, abuse Gmail's email forwarding function in order to successfully deliver emails classified

as spam by relaying them through white listed Gmail servers -- [now DomainKeys empowered](#) :

"The presented vulnerability enables an attacker to bypass blacklist/whitelist based email filters and freely forge all fields in an email message by having Google's SMTP servers tricked into behaving like open SMTP relays. We were able to confirm that this vulnerability is indeed exploitable by assembling a proof of concept (PoC) attack that allowed us to use one single Gmail account to send bulk messages to more than 4,000 email targets (which surpasses Gmail's 500 messages limit for bulk messages). Although we have limited the number of messages in our example to 4,000+, no counter measures took place that would have prevented us from sending more messages, and for that matter sending an unlimited number of messages."

What this means is that the potential spamming speed achieved through a single automatically registered Gmail account could be greatly increased. From another perspective, a bogus account wasn't worth as much as it is worth today, since it allows automatic access to all of the company's web properties allowing spammers and cybercriminals ([Cybercriminals syndicating Google Trends keywords to serve malware](#)) to abuse them even further. CAPTCHA is dead, humans that were supposed to recognize it killed it by starting to recognize it efficiently and monetizing the process.

The bottom line, ask yourself the following - how many **incoming** anti-spam solutions can you think of right now, and how many **outgoing** anti-spam solutions are you aware of? Before spam comes it has to go out first.

Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails | ZDNet

Brad Taylor, Google's Gmail Spam Czar, has just posted details on [the ongoing cooperation with PayPal and Ebay](#) , two of

the most targeted brands in phishing emails, the effect of which is rejecting compared to flagging as spam each and every email pretending to be coming from paypal.com and ebay.com as well as from their international domain extensions. It's a win-win-win move for users, and the companies themselves which are now digitally signing all of their emails, making phishing emails spoofing their origin easier to detect :

"Since 2004, we've been supporting email authentication standards including DomainKeys and DomainKeys Identified Mail (DKIM) to verify senders and help identify forged messages. This is a key tool we use to keep spam out of Gmail inboxes. But these systems can only be effective when high volume senders consistently use them to sign their mail -- if they're sending some mail without signatures, it's harder to tell whether it's phishing or not. Well, I'm happy to announce today that by working with eBay and PayPal, we're one step closer to stopping all phishing messages in their tracks.

Now any email that claims to come from "paypal.com" or "ebay.com" (and their international versions) is authenticated by Gmail and -- here comes the important part -- rejected if it fails to verify as actually coming from PayPal or eBay. That's right: you won't even see the phishing message in your spam folder. Gmail just won't accept it at all. Conversely, if you get an message in Gmail where the "From" says "@paypal.com" or "@ebay.com," then you'll know it actually came from PayPal or eBay. It's email the way it should be."

As Google put it - it's been working so well that you wouldn't be able to notice it. Moreover, despite that Sender ID and DomainKeys Identified Mail are well known concepts for validating the sender, and consequently capable of blocking huge percentage of emails that

pretend to have been sent from legitimate emails, just like [DNSSEC](#) which emphasizes on authenticating DNS data, it's all a matter of implementation on a large scale. Or the lack of.

According to the Authentication and Online Trust Alliance's (AOTA) "[State of Email Authentication and the Internet Trust Ecosystem 2008](#)" report, the adoption of trusted sender practices by major U.S ISPs and email providers is increasing :

"Over 700 million mailboxes are now protected by email authentication thanks to adoption by leading ISPs including AOL, Bell Canada, GoDaddy.com, Google (Gmail), Microsoft (Windows Live Hotmail), and Yahoo!. However, there is considerable room for improvement in the adoption rate amongst all ISPs. As a best practice, ISPs are encouraged to begin to delete or block email which fails authentication, rather than placing it in bulk or junk email folders where consumers remain at risk of disregarding warnings and opening the email."

Windows Live Hotmail also claim to block over 25 million deception emails daily using the Sender ID Framework :

"According to a study by Windows Live Hotmail, SIDF has contributed to an 8% reduction in spam, the detection of over 25 million additional deceptive emails per day, and upwards of an 85% improvement in deliverability for brands that authenticate and have a positive reputation."

Are DomainKeys and Sender ID the panacea of dealing with spam? Not necessarily, since spammers and phishers will always adapt to the situation given the incentives they have to do so, and ISPs on the other side, are showing no interest in taking care of their malware infected customers. At the end of the day, it's these malware infected customers whose bandwidth gets abused for sending out phishing and spam emails.

A safer Gmail doesn't mean less spam on the Internet if we are to consider the big picture - like we should. And as we've seen already, phishers and spammers are working on ways to start abusing the *authenticated* and digitally signed email service providers, by [breaking their CAPTCHAs and pre-registering hundreds of](#)

thousands of bogus email accounts in order to improve their delivery rates.

German ministers advised to dump BlackBerry for security reasons | ZDNet

Citing the potential for "political IT attacks", following the ongoing bargaining between [RIM and Middle East countries on improving lawful surveillance](#), Germany's Interior Minister is [advising ministers to dump the BlackBerry](#), and replace it with [BSI-certified SiMKo 2](#) smart phones.

What's so special about the SiMKo 2 device from a security perspective?

First introduced in [2009's CeBIT](#), the smart phone is exclusively marketed to government agencies, and has been recommended by the Federal Office for Information Security (BSI), for handling Classified – for official use only (VS-NfD security level) data. Following its release, [the device was quickly adopted by German ministers](#), clearly not to extend as recommended for the country's Interior Minister:

BlackBerry's infrastructure is a company-owned closed system. But the access standard must be capable of being set by the government and not by a private company.

From data encryption, standard S/MIME, digital identities through certificates (microSD based hardware tokens), VPN tunneling, what's particularly interesting about the device is that, T-Systems have labeled the camera, bluetooth, GPS and WLAN as potentially unsafe, and has consequently deactivated the interfaces. With all interfaces other than GSM, EDGE and UMTS disabled, and [VPN tunneling enforced by default for EDGE and UMTS data transfers](#), the device clearly aims to offer secure end-to-end data transfers.

Go through related resources on BlackBerry's security features:

[BlackBerry Security Features Advanced Security Features for Government BlackBerry Enterprise Solution - Security Technical Overview](#)

In 2007, [the French cabinet issued a similar ban](#) citing a two-year confidential study into the security of BlackBerry devices. Earlier this year, the French cabinet found an alternative solution, and adopted the [TEOREM phone](#). U.S President Barack Obama, also faced a similar situation when he wanted to keep his BlackBerry, but was given [a Sectera Edge device](#).

What the three devices currently share, though, is a ubiquitous flaw which no OS-hardening process -- unless it kills the core functionality of the device in the face of communication -- can protect against - the end user.

Georgia President's web site under DDoS attack from Russian hackers | ZDNet

From Russia with (political) love? It appears so according to a deeper analysis of the command and control servers used by

the attackers. During the weekend, [Georgia President's web site was under a distributed denial of service attack](#) which managed to take it offline for a couple of hours. The event took place in a moment of [real life tensions between Russia and Georgia](#), with Russia clearly demonstrating its position against Georgia's pro-Western government. Shadowserver's comments, which originally picked up the attack first :

"For over 24 hours the website of President Mikhail Saakashvili of Georgia (www.president.gov.ge) has been rendered unavailable due to a multi-pronged distributed denial of service (DDoS) attack. The site began coming under attack very early Saturday morning (Georgian time). Shadowserver has observed at least one web-based command and control (C&C) server taking aim at the website hitting it with a variety of simultaneous attacks. The C&C server has instructed its bots to attack the website with TCP, ICMP, and HTTP floods. Commands seen so far are:

```
flood http www.president.gov.ge/ flood tcp www.president.gov.ge  
flood icmp www.president.gov.ge
```

The server [62.168.168.9] which houses the website has been largely offline since the attack started. Passive DNS records show the system houses several other websites which are mostly unrelated to the Georgian government. However, the server does also host the Social Assistance and Employment State Agency website (www.saesa.gov.ge). This website along with the others on the host have been rendered inaccessible.

We do not have any solid proof that the people behind this C&C server are Russian. However, the HTTP-based botnet C&C server is a MachBot controller, which is a tool that is frequently used by Russian bot herders. On top of that the domain involved with this

C&C server has seemingly bogus registration information but does tie back to Russia. "

Russia's most recent cyber attacks successfully attacking [Estonia](#) , [Lithuania](#) and now Georgia, all share a common motivation despite that these attacks are executed from different parties, with Estonia still remaining the only coordinated attempt to attack a country's Internet infrastructure next to Lithuania and Georgia's lone gunman attacks.

The DDoS against Georgia President's web site appears to be using a well known Russian malware variant from the Pinch family -- whose [authors got arrested](#) after operating for several years online in 2007 -- next to a command and control bot (MachBot controller) primarily known to be popular in Eastern Europe, and including [messages in the flood packets like "win+love+in+Rusia"](#) , speak for itself. It's also interesting that despite that they've dedicated a new command and control server to be used specifically for this DDoS attack, one that haven't been seen in any third-party attacks, they made a small mistake further confirming the attacks has been launched by well known Russian botnet masters. Their mistake? Having the malware phone back to a well-known command and control seen in a great number of previous attacks, sharing DNS servers with a [provider of DDoS attacks on demand](#) , which despite announcing on its site that is no longer in business, continues offering [botnets for rent services](#) .

Russia's politically motivated, or perhaps politically tolerated attacks, are all the result of Russia's IT underground self-mobilization, feeling obliged to sent out a signal that they're in fact actively participating in the political life and monitoring everything. Moreover, [nationalistic articles in Russian newspapers](#) often further fuel the tensions and literally seek involvement from Russian hackers, so even when they speculate about non-existent hacker discussions on coordinated attacks against a particular country, such discussions actually start taking place and the result has been pretty evident ever since.

[Machbot command and control locations](#) image courtesy of Team Cymru.

Gawker Media tricked into featuring malicious Suzuki ads | ZDNet

A group of cybercriminals have [successfully managed](#) to trick [Gawker's ad sales team](#) into featuring [malicious ads serving Adobe exploits](#) ([CVE-2008-2992](#) ; [CVE-2009-0927](#)) and scareware, by [impersonating](#) a legitimate ad agency inquiring about an [upcoming Suzuki ad campaign](#) .

According to Gawker Media, the malware distributors were one of the most convincing ones they've seen, with clear experience in ad sales lingo. Here's a brief [chronology of the correspondence](#) between Gawker and the scammers, and what could Gawker media have done in order to [prevent the malvertising attack](#) :

"- Someone is approaching publishers as a representative of Spark-SMG on the Suzuki account, even though Suzuki very recently switched agencies - George Delarosa and his accomplice Douglas Velez claim that there's a limited amount of money left in the Suzuki account for them to spend, and they need to spend it quickly - They have intimate knowledge of online ad sales, including terms like eCPM, roadblocking, RON, IAB sizes, lead generation, traffic coordinators, etc. - Email comes from @spark-smg.com instead of @sparksmg.com, though the who-is for their spoof domain is very close to the actual domain (Erin has links in her original email) - They maintain a Chicago area code (where Spark is based) but claim to be in London, even though they couldn't give us the actual time in London when asked - Unlike most spammers, these guys were happy to jump on the phone to get ads back up and running - Clue that should have tipped us off was that we had to use our IO template...most major agencies like Spark have their own IO template"

A simple Google search for **Spark Communications** , followed by click on the "I'm feeling lucky" button would have revealed the true nature of typo-squatted and registered on the 4th of September, 2009, **spark-smg.com** domain that the cybercriminals used.

Go through related posts: [The ultimate guide to scareware protection](#) ; [MSN Norway serving Flash exploits through malvertising](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Scareware pops-up at FoxNews](#) ; [Ukrainian "Fan Club" Features Malvertisement at NYTimes.com](#)

A [similar social engineering attack](#) took place last month, this time featuring a scareware-serving malicious ad at the New York Times web site through a bogus Vonage ad. Clearly, [suspicion, and due diligence on prospective advertisers](#) can make an impact unless of course efficiency in the ad sales process gets higher priority than the safety of the site's users.

Despite that the participating malware sites in the Gawker campaign (**wbavv .com** , **criofree .com** , **bestavv .com** , **avcvv .com** , **avpgo .com** and **floweragents .com** , all parked at Latvian-based Telos Solutions LTD - 91.212.127.225) are currently down, the malvertising concept remains in the arsenal of cybercriminals to take advantage of in the long term.

FTC issues refunds to scareware victims | ZDNet

Have you been a victim of [scareware](#)?

If so, there's a high probability that a refund is waiting for you, just around the corner.

The US Federal Trade Commission announced that it plans to [issue refunds](#) to 320,000 known scareware victims, following a [settlement](#) with [Innovative Marketing](#)-- a producer and distributor of fake security software known as Winfixer, Drive Cleaner, and XP Antivirus. -- for \$8,272,962.

[With \\$100 million in revenues](#), Innovative Marketing's case clearly indicates just how profitable the scareware business is.

From Russia with (objective) spam stats | ZDNet

It's not every day that I get the chance to speak with a representative from the [Russian Association of Electronic Communications \(RAEC\)](#).

Especially, with one who's publicly admitting that based on their recently released study, not only are seven of world's top ten spammers Russians, but also, that [the world's number one spammer is a Russian](#) who lives in Moscow.

Here are the key findings from their study, and the summary points based on my conversation with RAEC's head of PR, Dmitry Zakharov.

Seven of the top 10 spammers are Russian
The world's biggest spammer is Russian, lives in Moscow and controls the biggest spam network selling pharmaceuticals over the Internet

Russian spammers earned 3.74 billion rubles (\$127 million) in 2009
The Russian economy lost 14.1 billion rubles (\$479 million) in reduced working hours in 2009

One-fifth of all Russian Internet advertisements is spam
US-based servers are responsible for 17.3 of worldwide spam, ahead of any other country

16.4 percent of Russian spam originates from servers based in the US

Some 83 percent of spam messages are sent by 'botnets', armies of zombie computers, based at home and in the office

Adverts for harmful, counterfeit Viagra are responsible for 73.7 percent of spam worldwide

So far, so good, in the sense that 50% of the problem is always solved by admitting it first.

What their research aims to emphasize on, is that whereas the world's top spammers are Russians, they are abusing U.S based infrastructure ([Research: 76% of phishing sites hosted on](#)

[compromised servers](#)) for their malicious operations, which depending on the nature of their malicious operations, will also utilize the network infrastructures of many other countries to accomplish their tasks using botnets.

The true value of the conversation lies within the conversation we had beyond the findings in their press release. Here are the highlights of it:

Spammers make more money, than they are fined with - According to RAEC's study based on publicly obtainable data of fines against EU based spammers, in 2009 the fines (€2.85 million) represented slightly more than 1% of their profits (€218 million). The same situation is often seen in different markets, where the companies engaging in illegal activities are in fact making so much money, that they can afford to pay the fines imposed on them. However, despite the obvious need of higher fines for spammers, from my perspective, imposing those fines on a participant within an affiliate network, in situations where you cannot get to the masterminds of it, undermines its effectiveness.

Russian cybercriminals are ahead of the legal framework - With [anti-spam legislation in Russia](#) virtually non-existent, it's no surprise that so many people are operating in the open, without any feeling of prosecution. However, another paradox we talked about, was the fact that some Russian spammers and cybercriminals in general, operate their campaigns outside Russian, in countries with developed anti-spam and anti-cybercrime laws. Yet, they are still at large.

The world's top spammers are Russian citizens, relying on U.S based infrastructure for their operations - Whether it's the systematic abuse of legitimate email providers ([Gmail, Yahoo and Hotmail systematically abused by spammers](#)), or compromised web sites, numerous independent studies continue emphasizing on this fact. For instance, the recent [PhishTank's stats for February, 2010](#) , and [MarkMonitor's Brandjacking Index for 2009](#) , both, point out that the U.S is hosting the majority of phishing sites. What does this mean? It means that from a pragmatic perspective, given the active legal framework, resources and technical capabilities, spam and

phishing shouldn't be the kind of problem it currently is. That's, of course, in a perfect world.

Spam and cybercrime in general are not a country-specific problem, but an international one - Although this is a fact and we both agreed on, another fact cannot be disputed - Eastern European based cybercriminals going after financial data, make Chinese cybercriminals look like cartoon heroes on their way to steal your virtual goods.

Go after the people, not the ISPs, as a form of public statement - The fact that there are people known as "spam kings" or "spam czars" means that they've been in operation for years. Moreover, based on the scale of their spam operations, and the money they make, a logical move on their behalf would be to keep a very low profile, and take basic operational security measures in place. That's not the case, making it easier to go after them.

Try to get to the top of the affiliate network chain, instead of prosecuting/fining a participant in the affiliate network - Who's getting prosecuted for spamming at the end of the day? It's usually not the one who should be. The next time you hear that a spammer has been arrested, is being sued, and possibly even fined, ask yourself the following - is this guy the one running an affiliate network with hundreds of thousands of spammers participating in it, the supplier of the counterfeit pharmaceuticals, or is he basically one of the thousands of participants in the network?

Several of my questions, however, remained unanswered. For instance - **Why are some of the Russian affiliate networks for spam already celebrating their 5th or 8th anniversaries?**

The lack of answer to this question is the result of a cybercrime ecosystem that was allowed to scale internationally throughout the years, ultimately leading to today's situation, where spam services as now a commodity sometimes offered as a bonus for doing business with an illegal enterprise.

Consider going through related posts: [Inside an affiliate spam program for pharmaceuticals](#) ; [Spamming vendor launches managed spamming service](#)

What do you think? Would the socially-oriented ambitions of the private sector, get undermined by the lack of active cooperation with law enforcement, next to the overall lack of political will to solve the problem internationally? Or is [RAEC's](#) research a light in the tunnel, following the recent [tightening of the procedures for registering a .ru domain](#) ?

Does it take an internationally successful identity theft ring ([Russia arrests three over \\$9m RBS WorldPay scam](#)), for Russian law enforcement to start taking actions?

TalkBack.

French hacker gains access to Twitter's admin panel | ZDNet

UPDATE2 : [Twitter confirms the unauthorized access](#) .

UPDATE : The Twitter admin hack appears to be the result of a successful social engineering attack against one of Twitter's employees -- [similar attack](#) took place in January this year. Here's a [retrospective of the events that took place](#) .

Yesterday, a French hacker claimed to have gained access to Twitter's administration panel, and based on the [screen shots that he included featuring internal data](#) for accounts belonging to U.S President Barack Obama, Britney Spears, Ashton Kutcher, and Lily Allen, as well as a detailed overview of different sections behind the scenes of Twitter, his [claims seem pretty legitimate](#) .

The hacker going under the handle of [Hacker Croll](#) featured [13 screenshots of Twitter's admin panel](#) , and commented that *"The images were taken from the Admin area that was secured with .htaccess. "* It's still unclear whether any data belonging to account holders was modified, but one has to assume that given the access obtained, there's a high chance that he was able to download anything he wanted to.

The attack comes two weeks after [multiple variants of Mickey's XSS worm](#) hit the continuously growing micro-blogging service.

UPDATE: [The screenshots were obtained](#) through the account of a Twitter employee who reported that his Yahoo! Mail account got compromised on the 27th - *"[Wow - my Yahoo mail account was just hacked.](#) "; "[If anyone with Yahoo! Security is out there, hit me up with an reply](#)."*

Interestingly, Hacker Croll goes into more details regarding the compromise on a different forum - *"one of the admins has a yahoo account, i've reset the password by answering to the secret question. Then, in the mailbox, i have found her twitter password. "* and that he *"used social engineering only, no exploit, no xss vulnerability, no backdoor, no sql injection "*.

Similar password reset attack contributed to the [successful hacking of Sarah Palin's personal email account](#) in September last year.

French gaming site serving ZeuS crimeware for over 8 weeks | ZDNet

Cybercriminals are constantly scanning the Web for exploitable and misconfigured web applications, and blogging platforms such as Wordpress for instance.

Not surprisingly, [hundreds of thousands of legitimate web sites remain susceptible to remote exploitation](#), which on the majority of occasions are serving malicious content to unsuspecting end and corporate users.

[According to researchers from Avast](#), the high trafficked **Assassinscreedfrance.fr** web site, has been serving ZeuS crimeware variants to its visitors for over 8 weeks. Moreover, the researchers point out that the web site is among the remaining 1,841 legitimate web sites serving the same crimeware variant.

The web site is currently returning a *"Parse error: syntax error, unexpected T_CONSTANT_ENCAPSED_STRING in /homepages/23/d207590046/htdocs/wp-content/plugins/countdown-timer/fergcorp_countdownTimer.php on line 1050"* error message.

How did the malicious attackers obtained access to the affected gaming web site? By exploiting the outdated Wordpress version running on this domain. Avast is also confirming that based on an analysis of 6000 affected .com web sites, a huge percentage of them are susceptible to exploitation through outdated and vulnerable Wordpress plugins.

Users are advised to keep an eye for newer version of the popular blogging platform, including the introduction of new versions of the [Wordpress plugins](#) currently in use by their web sites.

French E-voting portal requires insecure Java plugin | ZDNet

Imagine you're an ordinary citizen who wants to vote online. As an IT security conscious user knowing that in 2012 the [majority of vulnerabilities are found in third-party applications compared to Microsoft's products](#), you regularly check [Mozilla's Plugin Check](#) service to ensure that you're not using outdated browser plugins exposing you to client-side exploitation attacks served by web malware exploitation kits.

What seems to be the problem? [According to Benoit Jacob](#), the problem starts if you're a French citizen wanting to vote online, as the country's E-voting portal currently [doesn't support the latest version of Java](#). If that's not enough, the portal recommends users to switch to an alternative browser since Firefox blocks older Java plugins for security reasons, or use the insecure Java version 1.6.0_32.

What we've got here is a great example of a security trade off. Basically if you want to vote online you would have to expose yourself to the client-side exploits targeting older Java versions.

The administrators behind the E-voting portal could not be reached for a comment. Let's hope the situation will be resolved soon.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Foxit Reader intros new Safe Reading feature | ZDNet

With numerous reports, continuing to highlight [the rise of malicious PDFs](#), in combination with [DIY crimeware tools acts as a key driving force](#) for the growth of cybercrime, end users and companies are constantly looking for ways to mitigate the risks posed by the ubiquitous PDF format.

This week, Adobe's main competitor in respect to the timely introduced security features responding to in-the-wild threats, has once again reacted to the current cyber threat landscape, by introducing a new feature in the [latest Foxit Reader v3.3](#).

More details on the new feature, including a test using a spamvertised [malicious PDF relying on the /Launch command](#) :

The Foxit Reader 3.3 enables users to allow or deny unauthorized actions and data transmission, including URL connection, attachments PDF actions, and JavaScript functions; efficiently avoiding the attack from malicious contents and viruses. Enables users to show or hide the Ask Search Button in the Preferences menu.

The "*Enable Safe Reading Mode*" feature is not just alerting the end user, it's actually preventing any further interactions with the malicious PDF file. This is where the true usefulness of the feature really is, as you can see in the attached screenshot, using a spamvertised malicious PDF file, using the "/launch" command.

For a truly safe, PDF format experience, disabling JavaScript Actions from Tools -> Preferences -> JavaScript -> Disable JavaScript Actions, is also highly recommended.

Windows users running the Foxit Reader, in a combination with well configured [NoScript](#) for Firefox, [least privilege accounts](#), decent [host-based firewall](#), lack of any [outdated third-party applications](#) on their host, and [sandboxing /isolated web browsing](#) habits, mitigate a huge percentage of the currently active exploitation tactics used by cybercriminals.

So, what are you waiting for? The time has come to migrate to an alternative PDF reader.

Four XSS flaws hit Facebook | ZDNet

Project XSSed, the clearing house for cross site scripting flaws has just [released details on four flaws affecting Facebook's](#) developers page, iPhone login page and the new users registration page, potentially assisting malicious attackers into adding more legitimacy to their campaigns. With yet [another critical XSS flaw hitting Facebook in May](#) earlier this year, what's the potential exploitability of such flaws if any in the wake of the ongoing [Koobface worm's](#) rounds [across the social networking site](#) ?

It's worth pointing out that in both of these cases there were no known cases of active exploitation, perhaps due to Facebook's quick reaction upon being notified of them. The very same lack of active exploitation was also present in several other cases throughout the year, namely, the [recent XSS affecting Google's login page](#) , and the [multiple HSBC sites \(still\) vulnerable to XSS flaws](#) . And if we are to exclude the [XSS worm at Justin.tv which infected 2,525 profiles in July](#) , active exploitation of such flaws is no longer favored compared to the less noisy social engineering tricks exploiting the weakest link - the Internet user social networking with a false feeling of security.

Take Koobface for instance. It scaled so efficiency without exploiting any social networking site specific flaw, only through social engineering tactics forwarding the entire spreading process to the already infected user, which in a trusted environment of friends proved to be a successful form of spreading. Despite the possibility for active exploitation of such flaws in phishing and malware campaigns, cybercriminals appear no be no longer interested in such noisy approaches, at least not while attempting to spread malware across social networking sites. Among the main reasons for this is the fact that their entire campaign would be based on a single propagation vector, which when taken care of through technical means would render their campaign useless. Instead, just like the Koobface gang continues to do, they mix the social engineering vectors by abusing legitimate brands as redirectors to the malware infected hosts serving the fake YouTube videos.

The Web in general is an entirely different topic, since I can easily argue that the long tail of SQL injected sites can outpace the traffic that could come from a single high-page ranked site that's participating in a malware campaign. Case in point - the [recent Internet Explorer zero day flaw is currently being served through SQL injections](#) affecting vulnerable sites across the Web, a pretty [logical move on which I speculated](#) given the fact that it was originally used on Chinese forums and sites only.

For the record, the Facebook security team has been notified of the recently published flaws.

Fortune 500 companies use of email spoofing countermeasures declining | ZDNet

Here's a paradox - a technology originally meant to verify the sender of an email message for the sake of preventing

spoofed messages from reaching the network, still hasn't been embraced by the world's biggest companies despite being around for years, but is actively used by adaptive [spammers increasingly abusing legitimate services](#) in order to take advantage of their [identifiable email reputations](#) .

A recently conducted study by [Secure Computing's TrustedSource](#) reveals that, not only a mere 40% of the Fortune 500 companies use Sender Policy Framework and DomainKeys Identified mail, but also, that the ones who've implemented the countermeasures aren't fully taking advantage of protection mechanisms offered at the first place.

"Out of the 2008 roster of Fortune 500 companies, a mere 202 appear to be using any of the forgery countermeasures provided by SPF, DKIM, or similar implementations. This poses a stark contrast to [Sendmail's Survey](#) , claiming some 90% of Fortune 1000 companies, suggesting a sharp decline from Sendmail's reported 282 companies. To make sure our results were accurate, we decided against using a random sampling and instead put together a list of all 500 primary domains used by the Fortune 500 and query them.

A mere 202 companies, when you account for the companies running both technologies - 40% of the Fortune 500. To make matters worse, only 65 of the 167 companies using SPF included the -all policy, which causes a fail result to be sent if the IP address is not found explicitly in the policy."

And while the majority of Fortune 500 companies need to perhaps strategize better on how to built more authenticity in their communications and in fact prevent malicious attacks from reaching their mailboxes, spammers have been reportedly publishing SPF records since 2004, with [MX Logic conducting a study into the tactic](#) back then indicating that :

"In its preliminary study, MX Logic found that some spammers have embraced SPF in the hope that their unsolicited email messages will be viewed as more legitimate because the messages have an SPF email authentication record associated with them. In a sample of more than 400,000 unique spam email messages that passed through the MX Logic Threat Center from Aug. 29 through Sept. 3, 16 percent had published SPF records."

Things are a bit different today, with spammers as active participants in the cybercrime ecosystem constantly demanding

fresh malware infected hosts, and having embraced outsourcing as a concept a long time ago, they seem to have stopped investing resources into building legitimate infrastructure themselves, but have started to either renting such on behalf of someone else who build it, or abuse that of legitimate email providers by bypassing their authentication in place allowing them to easily take advantage of the provider's trusted reputation.

Here's an example of spammers sending DomainKeys Identified Mail from Yahoo's SMTP servers in April, 2008, [found in a report issued by MessageLabs](#) , a practice made possible due to [the successful breaking](#) of these services [CAPTCHA based authentication](#) , either automatically or through human based CAPTCHA breakers :

"The spam mails are sent via SMTP using Yahoo!'s servers, ensuring the message is signed correctly using Yahoo! DomainKeys Identified Mail (DKIM). This is a sender authentication technique that uses a digital signature in the headers to indicate that the message is genuinely from Yahoo! and not spoofed as such. This approach further helps to ensure that mail generated in this way is harder to block using anti-spam methods based on the source IP address; as if it had been sent from genuine Yahoo! mail servers. In most cases the spam messages are routed through the premium Yahoo! "Plus" servers which are not listed in the Yahoo! webmail interface options page.

The Yahoo! accounts appear to have been generated programmatically, presumably defeating the Yahoo! CAPTCHA mechanism, because of the consistent format in all cases and all

have from-domain of @yahoo.co.uk currently. At the time of writing around 1,127 unique Yahoo! User IDs were used in the distribution of this latest type of spam over 28 days, with around 40 new IDs per day being generated."

As always, it's never been about the lack of technological solutions to eradicate all the junk and malicious emails hitting an organization's mailboxes and its customers. It's always been about the lack of implementation of these solutions, and ensuring that abusing the now trusted services isn't done as efficiently as it is for the time being.

Firefox 14 fixes 5 critical security vulnerabilities | ZDNet

The newest version of Mozilla Foundation's flagship Firefox browser [fixes 5 critical security vulnerabilities](#).

More details on the patched vulnerabilities:

- [MFSA 2012-56](#) - Code execution through javascript: URLs
- [MFSA 2012-55](#) - feed: URLs with an innerURI inherit security context of page
- [MFSA 2012-54](#) - Clickjacking of certificate warning page
- [MFSA 2012-53](#) - Content Security Policy 1.0 implementation errors cause data leakage
- [MFSA 2012-52](#) - JSDependentString::undepend string conversion results in memory corruption
- [MFSA 2012-51](#) - X-Frame-Options header ignored when duplicated
- [MFSA 2012-50](#) - Out of bounds read in QCMS
- [MFSA 2012-49](#) - Same-compartment Security Wrappers can be bypassed
- [MFSA 2012-48](#) - use-after-free in nsGlobalWindow::PageHidden
- [MFSA 2012-47](#) - Improper filtering of javascript in HTML feed-view
- [MFSA 2012-46](#) - XSS through data: URLs
- [MFSA 2012-45](#) - Spoofing issue with location
- [MFSA 2012-44](#) - Gecko memory corruption
- [MFSA 2012-43](#) - Incorrect URL displayed in addressbar through drag and drop
- [MFSA 2012-42](#) - Miscellaneous memory safety hazards (rv:14.0/rv:10.0.6)

Users are advised to update to the latest version immediately.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

FIFA World Cup themed malware campaign spreads malicious PDF files | ZDNet

Researchers from Symantec are reporting on an ongoing [targeted malware campaign using a FIFA World Cup 2010 theme](#), in an attempt to trick end users into executing a malicious PDF file, [exploiting a recently patched flaw](#) in Adobe Reader.

More details on the campaign:

The attacker(s) have downloaded Greenlife's PDF document, and changed it to include malicious code. They then attempted to email the malicious PDF to a user in a major international organisation that brings together governments from all over the world. We should emphasise that [downloading the PDF from the Greenlife website](#) is perfectly safe at the time of writing this blog.

The attack makes use of a recently patched vulnerability in Adobe Reader – [CVE-2010-0188](#). The patch for this critical rated vulnerability was released by Adobe on February 16, 2010. Since then we have observed a large number of targeted attacks attempting to exploit this vulnerability. Proof-of-Concept exploit code is available in the Internet which is contributing to the large number of observed attacks. The exploit makes use of a flaw in the TIFF file parsing in Adobe Reader. In particular, a stack overflow is caused by inserting a TIFF image into the PDF with a specially crafted "DotRange" tag.

Anticipating the logical increase of FIFA World Cup 2010 themed malicious activity, last month, the company [released some stats showing the dynamics](#) of malicious sites and spam campaigns using the World Cup as theme.

With the event scheduled to take place in June, 2010, cybercriminals will be the first to take advantage of the anticipated traffic flow, coming from gullible bargain seekers ([Survey: Millions of users open spam emails, click on links](#)).

According to recent reports, [malicious PDF files not only comprised 80 percent of all exploits for 2009](#), but also, represent

[the preferred infection vector for targeted attacks](#) in general, for the first time ever surpassing the use of malicious Microsoft Office files.

Users should not just update their Adobe products, or perhaps even [consider an alternative PDF reader](#), if truly paranoid. They should take a [comprehensive approach when dealing with all the 3rd party applications and browser plugins](#) , currently installed.

FEMA's PBX network hacked, over 400 calls made to the Middle East | ZDNet

Someone's been chatting a lot during the weekend, but picking up FEMA's PBX network as their main carrier might not

have been the smartest thing to do. Over 400 calls, lasting from three up to ten minutes were placed through their network, a breach made possible due to an [insecurely configured Private Branch Exchange system](#) :

"A hacker broke into a Homeland Security Department telephone system over the weekend and racked up about \$12,000 in calls to the Middle East and Asia. The hacker made more than 400 calls on a Federal Emergency Management Agency voicemail system in Emmitsburg, Md., on Saturday and Sunday, according to FEMA spokesman Tom Olshanski."

Calls were placed to exotic locations such as Afghanistan, Saudi Arabia, India and Yemen, with Sprint originally detecting the compromise and blocking all outgoing long-distance calls from the location. If you're to assume a zero day vulnerability was used in process you'd be wrong as an unpatched vulnerability is just as useful as a zero day one :

"At this point it appears a "hole" was left open by the contractor when the voicemail system was being upgraded, Olshanski said. Olshanski did not know who the contractor was or what hole specifically was left open, but he assured the hole has since been closed."

With no shortage of vulnerabilities allowing automated reconnaissance for easily exploitable systems to happen, perhaps if you were to assume that you would be targeted "in between" next to being exclusively targeted this wouldn't have happened, as I doubt this phreaker knew he was using FEMA's network in the first place.

Federal Reserve themed emails lead to ZeusS crimeware | ZDNet

Researchers from Barracuda Labs have intercepted a [currently spamvertised malware campaign](#) serving the ZeusS crimeware.

Sample subject: *Your Wire fund transfer*

Sample attachment: *federalreserve.report.pdf.exe*

Sample message: *The outgoing Wire fund transfer, a short time ago sent from your banking account, was not processed by the Federal Reserve Wire Network. Please click here to view further information.*

Upon downloading the executing the crimeware, users are automatically exposed to E-banking session hijacking attacks, and general theft of accounting credentials.

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Federal forms themed blackhat SEO campaign serving scareware | ZDNet

An ongoing blackhat SEO (search engine optimization) campaign is actively hijacking a variety of [U.S Federal Forms](#) keywords in an attempt [to serve](#) the Personal Antivirus (Trojan.Win32.FakeXPA) [scareware](#) .

Due to the automated and sophisticated PageRank boosting tools cybercriminals use in these campaigns, the hijacked keywords are always popping-up within the first ten to twenty search results for a given keyword.

Let's analyze the campaign, and discuss how are they capable of bypassing Google's SafeBrowsing blacklist.

Compared to previous real-time ([news headlines](#) and [swine flu themes](#)) blackhat SEO campaigns launched during the last couple of months, this one is relying on a pre-defined set of legitimate applications and U.S Federal forms. The following list is a sample of some of the keywords used:

Irs 8905, Printable Ohio Individual Tax Form, Wisconsin State Amended Tax Form, It 1040 Ohio Form, Federal 1040ez Form, 1040 Ez Online Form, Wi 1040 Ez, 1040 Tax Form Download, Virginia Health Life Insurance License Form, Commercial Lease Offers Application Form, Free Medical Durable Power Of Attorney Form, Georgia Driving History Request Form, Parcar Warranty Claim Form, Uc 101 Form, Estate Waiver Form, Postnuptial Agreement Form, 403 B Salary Reduction Form, Copy Of Living Will Form Fl, Petition Divorce Form Oklahoma Free, Rental Agreement Form Oregon, Alaska Form Expected Death At Home, Application Form For Callas Reward Card, Celebrities Form Bretagne France, Annual Emeritus Parking Authorization Form, 540ez Ca, Illinois State Form 1040, Ira Form 8863, Income Tax Return 1040ez Form, 1096 Form Tax, Kerala Medical Examination Form, Cayman Islands Visa Form, Ohio Tax Exemption Form, Free Printable Tax Forms 1099, 1040 Tax Form Printable, Gsa Form 3503 Form Fillable, Change Of Schedul

Form 3189 Uspostal, Medical Treatment Form Ohio, Default Form Louisiana Parish Preliminary Vernon, Client Interview Form Unlawful Detainer California, Nonresident Form Hawaii Vehicle

Based on the variety of keywords used, it's pretty obvious the cybercriminals behind it are attempting to exclusively hijack U.S traffic.

Go through related posts showcasing the use of blackhat SEO for malicious purposes: [Cybercriminals hijack Twitter trending topics to serve malware](#) ; [Cybercriminals promoting malware-friendly search engines](#) ; [The Web's most dangerous keywords to search for](#) ; [Cybercriminals syndicating Google Trends keywords to serve malware](#) ; [Google Video search results poisoned to serve malware](#)

It's worth pointing out that they've apparently managed to trick Google's Safebrowsing blacklist on the true nature of the sites' content. How did they do that?

By using some well known evasion practices in their arsenal, in this case it's a combination of web content cloaking and http referrer checking. Basically, they detect a Google crawler and serve legitimate blackhat SEO optimized content to it, however, since the crawler isn't using a [http referrer](#) , the cybercriminals only serve the scareware to someone who's directly coming from Google's search engine, and a 404 error to those who are basically clicking on the links without a valid http referrer.

Disruption of the campaign is in progress.

FBI: Scareware distributors stole \$150M | ZDNet

Just how much money did scareware scammers steal from Internet users so far?

According to an intelligence note posted by the [Internet Crime Complaint Center \(IC3\)](#), the FBI is aware of an estimated loss to victims in excess of \$150 million. The number should be considered as a rough estimate of a much worse situation, with over [40 million people observed internationally, falling victim to rogue antivirus scams](#) in one year.

What is the IC3 emphasizing on in its intelligence note? The use of ["least privilege" accounts](#) as a [preventative measure](#) (sandboxing is an alternative).

"The scareware is intimidating to most users and extremely aggressive in its attempt to lure the user into purchasing the rogue software that will allegedly remove the viruses from their computer. It is possible that these threats are received as a result of clicking on advertisements contained on a website. Cyber criminals use botnets to push the software and use advertisements on websites to deliver it. This is known as malicious advertising or malvertising.

Once the pop-up appears it cannot be easily closed by clicking "close" or the "X" button. If the user clicks on the pop-up to purchase the software, a form is provided that collects payment information and the user is charged for the bogus product. In some instances, whether the user clicks on the pop-up or not, the scareware can install malicious code onto the computer. **By running your computer with an account that has rights to install software, this issue is more likely to occur. "**

The estimated financial losses to customers caused by scareware, greatly [outpace the revenues generated by spam](#) in general, which due to its epic proportions is wrongly considered as a largely profitable cybercrime endeavor. From a cybercriminal's perspective, the conversion rate of exposed and infected with scareware users,

looks much more favorable than the conversion rate of millions of users who clicked on a spam message, but purchased nothing.

What was the the single most important event that took place during 2009, and indicated the cybercrime underground's long-term ambitions into developing the scareware business model?

There are two actually - the integration of [the scareware business model](#) within each and every infected host [part of the Koobface botnet](#) which is still happening, and even more interestingly, the only [attempt by the Conficker botnet to engage in fraudulent activities](#) so far, by pushing scareware on already infected hosts.

You know that scareware is a "game changer", when the Conficker botnet decides to temporarily join the business model, instead of relying on spam campaigns as a revenue source.

Throughout the entire 2009, scareware successfully matured as a fraud scheme, and positioned itself as one of the most profitable monetization tactics applied by cybercriminals. The fraud tactic is prone to escalate in 2010 due to a single fact - it's profitable and the business model has already been [positioned as a cash cow in Cisco's Cybecrime Return on Investment Matrix](#) .

[Prevention is always better than the cure](#) , and scareware isn't an exception.

Fast-Fluxing SQL injection attacks executed from the Asprox botnet | ZDNet

The botnet masters behind the Asprox botnet have recently started SQL injecting fast-fluxed malicious domains in order to enjoy a decent tactical advantage in an attempt to increase the survivability of the malicious campaign. I first assessed [the Asprox botnet](#) in January, and again in April when it started scaling and diversifying its campaigns from fake Windows updates, to [fake Yahoo ecards](#), as well as [executable news items](#). A botnet crunching out phishing emails and spam as usual? Depends on the momentum. Automating the process of SQL injecting a large number of sites is one thing, SQL injecting fast-fluxed domains is entirely another. Secureworks comments on [the introduction of the SQL injection tool within the botnet](#) :

"As of yesterday, we observed the Asprox botnet pushing an update to the infected systems, a binary with the filename msscctr32.exe. The executable is installed as a system service with the name "Microsoft Security Center Extension", but in reality it is a SQL-injection attack tool. When launched, the attack tool will search Google for .asp pages which contain various terms, and will then launch SQL injection attacks against the websites returned by the search. The attack is designed to inject an iframe into the website source which will force visitors to download a javascript file from the domain direct84.com. This file in turn redirects to another site, where additional malicious javascript can be found. Currently the secondary site appears to be down, however it is likely that when successful, the site attempts to exploit the visitor's web browser in order to install additional copies of either Danmec, Asprox and/or the SQL attack tool."

Now comes the fast-flux. The latest massive SQL injection attack courtesy of the Asprox botnet, is this time using the **banner82 .com** domain which continues to be in a fast-flux mode, namely, it's simultaneously hosted at ten different malware infected IPs, with the IPs constantly changing. Let's illustrate this by taking a look at the

changing IPs responding to the same domain within a period of 24 hours :

Fast-flux has been extensively researched by the HoneyNet Project, whose research into the topic greatly illustrates [single and double-fluxed networks](#) , with the Storm Worm acting as a personal benchmark for [the true dynamic nature of fast-flux networks](#) . Fast-flux was embraced by the malicious parties around the middle of 2007, when [managed fast-flux providers](#) appeared, and more [spam and phishing domains were set in a fast-flux mode](#) . Fast-fluxing SQL injected domains is, however, a new tactic, so you have a botnet of infected hosts that automatically scan and inject malicious domains within vulnerable sites, and the malicious domains themselves part of a fast-flux network provided by the botnet's infected population, that are also hosting and sending the phishing campaigns.

What is the objective of the latest SQL injection attack launched by the Asprox botnet? It's infecting new hosts to be added to the botnet. **Banner82 .com** has a tiny iFrame that's attempting to load **dll64 .com /cgi-bin/index.cgi?admin** where the NeoSploit malware exploitation kit is serving MDAC ActiveX code execution (CVE-2006-0003) exploit.

Here are sample fast-fluxing DNS servers used by **banner82 .com** , as well as a sample internal fast-flux structure used by the botnet:

```
exportpe .net ns1.exportpe .net ns2.exportpe .net ns3.exportpe
.net ns4.exportpe .net ns5.exportpe .net ns6.exportpe .net
ns7.exportpe .net ns8.exportpe .net
```

```
cookie68 .com ns1.cookie68 .com ns3.cookie68 .com
ns4.cookie68 .com ns4.cookie68 .com ns6.cookie68 .com
ns7.cookie68 .com ns8.cookie68 .com
```

```
ns1.ns2.ns4.ns1.ns7.ns8.ns1.ns4.ns6.ns3 .aspx88.com
ns1.ns2.ns4.ns6.ns7.ns7.ns3.ns2.ns5.ns1 .aspx88.com
ns1.ns2.ns5.ns1.ns7.ns8.ns2.ns5.ns4.ns3 .aspx88.com
ns1.ns1.ns5.ns2.ns7.ns8.ns1 .bank11.net
ns1.ns1.ns5.ns2.ns8.ns7.ns4 .bank11.net
```

The screenshots speak for themselves, and for the infrastructure they've managed to build using the malware infected hosts to send scams, host the scam domains, infect new hosts, scan for vulnerable sites, SQL inject them and host the live exploit URIs within. And with the introduction of fast-flux whose infrastructure is provided by the botnet's infected population, and automating the SQL injection process, the Asprox botnet is slowly turning into a self-sustaining cybercrime platform.

Go through [a related assessment](#) if you're interested in knowing more about the geographic locations of the infected hosts used in a sample SQL injection attacks, as well as related comments on [the use of botnets to launch SQL injection attacks](#) .

Fake YouTube sites target Syrian activists with malware | ZDNet

Cyber spies are constantly looking for new social engineering tricks in an attempt to trick anti-government activists in authoritarian regimes to install malware on their PCs.

Some of their tactics include the [automatic syndication of relevant content](#) for building blackhat SEO content farms where the bogus content will attract unsuspecting visitors into clicking on malware-serving links.

The Electronic Frontier Foundation (EFF), has recently spotted a [fake YouTube site that's serving malware to Syrian activists](#).

The web site is a combination of a phishing site, and malware-serving site, enticing end user into logging in with their YouTube credentials in order to post comments, or tricking them into installing a bogus Adobe Flash Player update in order to view the video.

What's particularly interesting about this attack, is the fact that the content has been localized to the native language of the prospective victims. Localization within the cybercrime ecosystem is emerging as a tactic of choice for a huge number of malware-serving malicious campaigns wanting to increase the probability of a successful infection.

Fake WordPress site distributing backdoored release | ZDNet

Can you find five differences between these two sites? Wordpresz.org may indeed look like WordPress.org , but the **2.6.4** release it's distributing is on purposely backdoored in order to steal the content of cookies from those who have installed it, potentially leading to hijacking of their WordPress blogging platforms for malicious purposes. Not only is the fake domain registered several days ago, but also, it's sharing IP (**209.160.33.108**) with a fake online pharmacy - **livepills.com** .

A [brief summary](#) by Sophos of [Craig Murphy's alert](#) issued on Monday :

"Craig talks about how when he logged in to his admin account in WordPress he received a "High Risk Vulnerability Warning" from a spoofed WordPress domain. (The last 's' in WordPress.org has been replaced by a 'z'.) The Warning suggests upgrading to the 'new' version 2.6.4 of WordPress. Downloading this 'new' version of WordPress I found that of the 638 files in version 2.6.4, 637 were identical to the same files in the official 2.6.3. The only difference was in the file `pluggable.php`. The hacked version of the file `pluggable` appears to be stealing the content of cookies on larger installations of WordPress. Sophos are now detecting this file as [Troj/WPHack-A](#) ."

The backdoored **`pluggable.php`** file attempts to send the stolen data to **`wordpress.org/tuk.php`** which is still accepting cookies if the requests are properly formatted. The spoof is a nearly perfect combination of social engineering, typosquatting and the natural [EstDomains connection](#) as the domain registrar, nearly perfect in the sense that they couldn't duplicate the whole WordPress.org potentially raising suspicion at the end user's end.

Fake Windows XP activation trojan goes 2.0 | ZDNet

Known as [Kardphisher](#) and "in the wild" since April, 2007, last week the malware author of this trojan horse mimicking the Windows XP activation interface while collecting the credit card details the end user has submitted, has made significant changes to visual interface and usability of the trojan, consequently improving its authenticity. Guess what happens when a gullible end user falls victim into this social engineering attack?

Their credit card details end up automatically into an IRC channel specifically set for that purposes. Some of changes in the new version include more legitimately looking color scheme, improved restrictions making it much harder for the end user to close the application without submitting their credit card details, [built-in validation of credit cards and email](#) , next to displaying the current product key to make the application look more legitimate. Once the user enters all the validated data, the new version of the tool automatically removes itself as if the activation was successful. Moreover, a bogus "verified by Visa" message that is also requesting social security number and a date of birth makes the trojan the perfect tool in the hands of identity thieves relying on nothing else but plain simple social engineering impersonating Microsoft.

The latest Kardphisher may indeed by filling in all the gaps from the previous version, but the trojan can never scale as efficiently as crimeware "in the middle" does for the time being. Among the main growth factors for the increasing number of such malware remains the fact that throughout the entire year proprietary crimeware kits costing several thousand dollars on average started leaking out, allowing many new entrants to start using what once used to be a highly exclusive tool in the arsenal of the experienced cybercriminal.

Fake 'Roar of the Pharaoh' Android game spreads premium-rate SMS trojan | ZDNet

Security researchers from Sophos, have spotted [a bogus Chinese game, that's actually a trojan horse](#) gathering sensitive information from infected devices, next to sending premium-rate SMS messages to multiple providers.

Once installed, the trojan horse will harvest the following information from the infected device (*IMEI, IMSI, phone model, screen size, platform, phone number, and OS version*), and will forward it to the malicious attackers operating it.

According to the vendor, the malware masquerades as a service called "*GameUpdateService* ", which sounds like a legitimate name for an application, yet another indication of the social engineering element part of the campaign, next to the actual brand-jacking of a legitimate game's name.

The malicious application is currently detected as Andr/Stiniter-A.

With independent third-party reports indicating a massive growth in the [distribution and production of mobile malware targeting the Android OS](#), the process of brand-jacking a legitimate game's brand, is among the many other tactics and techniques available at the disposal of the malicious attacker, looking for new and flexible ways to spread his malicious application.

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/>
and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back
these settings

CLOSE

Malicious Japan quake spam leads to scareware | ZDNet

[M86 Security](#) and [Kaspersky Lab](#) are reporting on a currently ongoing Japan quake themed spam campaign which leads to scareware and client-side exploits. Spammed using the Cutwail/Pushdo botnet, the campaign is using an event-based social engineering theme in order to trick users into clicking on the malicious links.

Upon clicking on the link the user is exposed to [client-side vulnerabilities](#), ultimately dropping a [scareware](#) variant.

[Millions of users continuing to clicking on links in spam emails.](#)

Meanwhile, users are advised to browse the Web in a [sandboxed environment](#), using [least privilege accounts](#), [NoScript for Firefox](#), and ensuring that they are [free of client-side exploitable flaws](#).

Major career web sites hit by spammers attack | ZDNet

What is the future of spamming next to [managed spamming appliances](#) , like the ones already offered for use on demand?

It's [targeted spamming going beyond the segmentation](#) of the already harvested emails on per country basis, and including other variables such as city of residence, employment history, education, spoken languages, to ultimately set up the perfect foundation for targeted spamming and malware campaigns.

Email harvesting has been around since the early days of spamming, when the handy point-n-click mailto made it possible for the first databases of harvested emails to appear. Nowadays, these lists either come as a commodity, namely, they're free, or as a bargain for enticing the buyer of a particular underground good or service into buying it, and receive the list as a bonus. Recently, [spammers, phishers and malware authors](#) , started diversifying their harvested databases that would be later on used as hit lists for spam and malware campaigns, from the usual emails, to [instant messaging screen names](#) , [Skype usernames](#) , and even [YouTube user names](#) . In fact, the problem of spammers diversifying their hit list building approaches is so prolific, that successful initiatives such as [the Project Honeypot](#) aiming to proactively detect such email harvesters and limit their reach, would need to diversify their distributed aggregation approaches in the long term, to include many other ways in which spammers are harvesting "contact points" on their watch list.

This post will assess a recently discovered in the wild, do-it-yourself proprietary email and personal information harvesting tool, outline its functions, list the career web sites targeted, and emphasize on how this attack would ultimately result in far more successful spamming, and targeted malware campaigns.

Key summary points :

the personal information harvesting tool comes with a customer service, which would provide the buyer with a custom module for any other web site included for the price of \$100, in between providing accounts at that site and lists of proxy/socks hosts to be used, and therefore speaks for a decent degree of customerization

the tool is entirely efficiency centered, namely, it allows multiple harvesting threads which in combination with several different socks/proxy hosts used can fetch and parse a huge number of pages in the shortest possible time frame

the service has a built-in proxy/socks functionality, allowing the spammers to forward the responsibility for the harvesting process to the owner of the proxy/socks which in most cases is a malware infected PC used as a stepping stone for committing other illegal acts

one of the main differentiation factors of this tool compared to the many other average email harvesters, is the customization achieved, namely the spammer can harvest only emails of people living in a certain country, city, working a specific profession, having studied in a particular school, or having worked in a particular company in the past, spoken language, possession of a security clearance, as you can see in the attached screen shots the variables for coming up with unique and highly targeted spamming lists fully match the variables for searching on a per job site basis

the possibilities for targeted spamming and malware attacks here are enormous given the quality of the harvested data, which compared to the plain simple email addresses spammers harvest, a situation where they have no idea about any other personal details of the email owner, in this security incident, the information in all of its authenticity and quality is provided by legitimate job seekers wanting to dazzle their future employers by providing them with as much information as possible

the tool relies on the already registered accounts at these sites, whenever it cannot recognize the CAPTCHA, and according to the description it can recognize the CAPTCHA of a single career site only, CAPTCHA images are parsed within the interface per session, so even if the CAPTCHA for a certain site cannot be automatically recognized, the spammer is verifying it successfully, thereby gaining

access inside the portal as a legitimately authenticated job seeker as it appears from the obtained log files, the tool has already been actively harvesting the job sites

Description of the do-it-yourself email harvesting tool:

"Your attention is invited to product-collector e-mails within web resources. By purchasing our product, you get free updates for life, the opportunity to use our hosting for the collection of e-mails. Many have already chosen our product and we are grateful. Product Price: \$ 600 Help with the installation - for free. It is possible to write custom modules - normal price is \$ 100 and the availability of the resource account for which you want to write a module. PHP Mailers for direct spamming come as a gift."

Sites targeted and included in the web application :

Ajcjobs.com ; CareerBuilder.com ; CareerMag.com ; ComputerJobs.com ; HotJobs.com ; JobControlCenter.com ; Jobvertise.com ; MilitaryHire.com ; Monster.com ; Seek.com.au

With the increasing information sharing between security vendors, non-profit

organizations and independent researchers, the pressure put on spammers, phishers and malware authors is prompting them to consolidate, and start exchanging resources and know-how. And while some of the participants will provide the [infrastructure for mass mailing the phishing and spamming emails](#) (malware authors), other would continue abusing the clean IP reputation of legitimate email services, where once they've managed to find a way to [bypass the CAPTCHA authentication process](#) , several hundred of thousands rogue email boxes would be registered. This particular scenario as a matter of fact represents the current situation, and basics of supply and demand in the underground market.

Out there right now, there's a legitimately registered user, whose access to a site is efficiently abused part of an illegal operation. It could happen at any site, at any time, not necessarily job sites only given that a custom module for any other site could be build as well. However, job sites were originally targeted in this incident because of the quality and easy to aggregate, personal information.

Here are several more related screen shots showcasing the rest of the tool's option.

A sample output in the form of full name and the associated email :

The variables to set before harvesting the email addresses :

Other variables for a specific career site :

Sample log file of the process :

The trend of obtaining high quality personal data from business social networks is only starting to take place.

Mac OS X SMS ransomware - hype or real threat? | ZDNet

In need of a fresh example that cybercriminals are actively looking for ways to monetize infected Mac OS X hosts?

Early-stage discussions at several web forums, including a PoC (proof of concept, source code included) Mac OS X blocker as well as potential GUIs for [the ransomware](#) , offer an insight into the potential to monetize OS X infected hosts using SMS-based ransomware.

Is Mac OS X ransomware just a hype, or a real threat? Let's take a brief retrospective of known OS X monetization strategies used by cybercriminals, discuss the ransomware threat on the Windows OS, and go through some pretty self-explanatory ransomware layouts for the OS X based ransomware.

What have originally started as a complaint from a single user who claims to have been victimized by SMS-based ransomware on his Mac OS X, motivated others to not just come up with possible layouts for the OS X ransomware GUI, but also, release a proof of concept blocker.

In its current version, the PoC blocker doesn't extort money, instead it demonstrates its ability to intercept all attempts to close down and exit the application, with the author and other participants commenting that "*although it was built as a PoC, anyone can add additional features including auto-starting features, perhaps even spreading functionality*".

Consider going through related ransomware posts: [iHacked: jailbroken iPhones compromised, \\$5 ransom demanded](#) ; [New LoroBot ransomware encrypts files, demands \\$100 for decryption](#) ; [New ransomware locks PCs, demands premium SMS for removal](#) ; [Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"](#) ; [Who's behind the GPcode ransomware?](#) ; [How to recover GPcode encrypted files?](#)

Sadly, they are right. And while the commonly shared attitude between the people participating in the discussion is in the lines of "*harmless joke having nothing to do with malware*", ransomware is virtual extortion, or the monetization of disrupting an end user's productivity. Another participant in the discussion is pretty straightforward in his ambitions by saying "*Guys, we are ready. Looking forward to it*".

Cybercriminals are no strangers to the Mac OS X ecosystem. From Mac OS X [affiliate bounties offering 43 cents per infected Mac](#) , the [monetization](#) of [Mac OS X traffic](#) , the use of [pirated application releases](#) , and good old fashioned [social engineering attempts](#) in the form of [fake codecs or missing plugins](#) , Mac OS X malware is no longer a myth. Ransomware, is perhaps the only segment of malicious software that hasn't been released on the Mac OS X so far.

How widespread is the ransomware threat on the Windows OS? Pretty widespread. According to [Fortinet's February Threatscape report](#) :

Most notable was the number one chart-topping malware variant, HTML/Goldun.AXT, which works by disseminating a binary malware file that downloads the ransomware "Security Tool" and, once executed, locks up applications until a cleansing tool is purchased to restore the computer. While this example accounts for the majority of activity detected this period, the Security Tool ransomware was also distributed through SEO attacks as well.

As in every other malware segment, an epidemic of a particular threat is often triggered by the overall availability of DIY (do-it-yourself) tools, or managed services allowing novice and potential cybercriminals easy access to tools and DIY malware kits. Throughout the entire 2009, the cybercrime ecosystem was actively developing the SMS-based ransomware market segment, but persistently releasing new layouts, and adding new features within ransomware releases available for sale.

Consider going through related Windows-based ransomware research: [SMS Ransomware Displays Persistent Inline Ads](#) ; [SMS Ransomware Source Code Now Offered for Sale](#) ; [3rd SMS](#)

[Ransomware Variant Offered for Sale ; 4th SMS Ransomware Variant Offered for Sale ; 5th SMS Ransomware Variant Offered for Sale ; 6th SMS Ransomware Variant Offered for Sale](#)

The laws of demand and supply fully apply within the cybercrime ecosystem. Therefore, it's only a matter of time before someone starts developing this malware segment, either driven by personal financial gains, or by someone else's demand for such a malicious release.

What do you think? Is Mac OS X ransomware a real threat, or a hype, with cybercriminals basically experimenting in the short term?

TalkBack.

Mac OS X malware posing as fake video codec discovered | ZDNet

Researchers from ParetoLogic are reporting on a [newly discovered Mac OS X malware variant posing as fake video ActiveX object](#) found at a bogus Macintosh PortTube site.

The use of [fake video codecs](#) is a social engineering tactic exclusively used by malware targeting Windows, and seeing it used in a Mac OS X based malware attack proves that successful social engineering approaches remain OS independent.

Prior to ParetoLogic's sample, [SophosLabs appear to have received](#) an email from the author of last month's discovered [OSX/Tored-A](#) sample, allowing them to add [generic detection](#) for any upcoming releases.

Here are some of the PornTube templates used in the social engineering attack, a description of the malware, as well the descriptive filenames used in some of the campaigns:

[OSX/Jahlav-C](#) is described as:

"OSX/Jahlav-C is a Trojan created for the Mac OS X operating system. The initial malicious installer is distributed as a missing Video ActiveX Object.

As a part of the installation a malicious shell script file AdobeFlash is created in /Library/Internet Plug-Ins folder and setup to periodically run. The script contains another shell script in an encoded format which in turn contains a Perl script with the main malicious payload. The perl script uses http to communicate with a remote website and download code supplied by the attacker."

The campaign is also using descriptive files such as, HDTVPlayer.v3.5.dmg; VideoCodec.dmg; FlashPlayer.dmg; MacTubePlayer.dmg; macvideo.dmg; License.v.3.413.dmg; play-video.dmg, and QuickTime.dmg.

What's Apple's take on this emerging trend?

Earlier this week, in a rare comment of potential [Mac OS X related insecurities in the face of malware](#) , the company not only acknowledged OS X Malware, but [also pointed out that](#) :

"The Mac is designed with built-in technologies that provide protection against malicious software and security threats right out of the box. However, since no system can be 100 percent immune from every threat, antivirus software may offer additional protection. "

Is the company finally taking the right decision to generate security awareness on a threat that is prone to become a daily routine in the long term, or was it too slow to stop using the Mac's massively advertised immunization to malware as a key differentiation factor?

What do you think?

Talkback.

Loozfon Android malware targets Japanese female users | ZDNet

[Security researchers from Symantec](#) have detected a [new Android trojan](#) currently circulating in the wild, attempting to socially engineer Japanese female users into downloading and executing the application on their mobile device.

What's particularly interesting about this Android malware, is that it also has a built-in spreading capability, namely, it sends spam stating that the sender can introduce the recipient to wealthy men. When users click on any of the links found in the emails, they're prompted to download a copy of the malware.

The application called “*Will you win?*” in Japanese, steals contact details, as well as the phone number of the malware. Why would a malware author want to collect the phone numbers of already infected devices? Pretty simple. The malware author is busy building a database of mobile phone numbers to be later on offered as a service to [prospective SMS spammers](#).

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Localized ransomware variants impersonate law enforcement agencies | ZDNet

[Security researchers from Microsoft](#), have intercepted multiple localized ransomware variants, impersonating law enforcement agencies across the world.

The researchers have intercepted samples using the following languages - English, Spanish, German, and Dutch.

Impersonated agencies include:

- The German Federal Police
- GEMA (Germany's performance rights organization)
- The Swiss "Federal Department of Justice and Police"
- The UK "Metropolitan Police"
- The Spanish Police
- The Dutch Police

According to their blog post, the infection rate for a corresponding localized ransomware coincides with the country in question. For instance:

In the case of [Trojan:Win32/Ransom.DU](#), which is a generic detection for a German-language variant of the ransomware that impersonates the German Federal Police, 91.59% of the samples we received from July to November this year were found in Germany, as we show in Table 1.

Is there a connection between these ransomware variants? According to Microsoft, a single gang is responsible for their release in the wild:

All the localized versions of the ransomware that we've encountered so far, except for the more recent GEMA case, have a very similar codebase. The HTML front-end has been translated, while the back-end stays almost the same, with the exception of some obfuscation layers. This fact indicates that they were created by the same gang, which has put some effort into designing an easy-to-localize solution.

How is the localization process taking place? Throughout the cybercrime ecosystem, [vendors of localization services](#) attract potential cybercriminals wanting to localize their spam templates and messages into specific languages, with valuable underground propositions aiming to satisfy their needs. The same goes for GUIs related to various programs, in this case ransomware variants.

In the past, we have seen the [localization of open source malware](#), including the [localization of scareware templates](#), and the localization of web malware exploitation kits such as [Icepack](#), [Firepack](#) and [MPack](#).

Localization is clearly growing as an underground market segment, offering easy market development and market penetration possibilities to cybercriminals looking for ways to target a wider audience.

Related posts:

[Microsoft themed ransomware variant spotted in the wild](#) [Copyright violation alert ransomware in the wild](#) [New ransomware locks PCs, demands premium SMS for removal](#) [Mac OS X SMS ransomware - hype or real threat?](#) [New LoroBot ransomware encrypts files, demands \\$100 for decryption](#) [Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"](#) [New ransomware variant uses false child porn accusations](#)

Localized ransomware variants circulating in the wild | ZDNet

Security researchers from **Abuse.ch** have intercepted multiple [localized ransomware variants](#) currently circulating in the wild.

The ransomware is dropped on the infected host using the [Black Hole](#) web malware exploitation kits, which exploits outdated and already [patched client-side vulnerabilities](#).

Once infected, end users are exposed to a professionally looking template impersonating a well known law enforcement agency in the targeted country, alerting they that their computer is locked due to the fact that "Illegally downloaded music pieces (pirated) have been found on their PC".

In their analysis, the researchers came across to templates localized to the native languages of the following countries:

Switzerland; Germany; Austria; United Kingdom; France and the Netherlands

Cybercriminals are no strangers to the concept of localization. Thanks for [managed localization and proofreading services](#) targeted exclusively to cybercriminals, the value-added practice from a QA (quality assurance) perspective is becoming increasingly popular among malware authors, spammers and phishers.

End and corporate users are advised to ensure that they're running the [latest versions of their third-party software](#), and [browser plugins](#) in an attempt to avoid getting exploited by the most popular exploit kit, the Black Hole web malware exploitation kit.

Related posts:

[New ransomware impersonates the U.S Department of Justice](#)
[New ransomware variants spotted in the wild](#) [Localized ransomware variants impersonate law enforcement agencies](#) [Microsoft themed ransomware variant spotted in the wild](#) [Copyright violation alert ransomware in the wild](#) [New ransomware variant uses false child](#)

porn accusations Mac OS X SMS ransomware - hype or real threat?
Who's behind the GPcode ransomware?

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Localized Dorkbot malware variant spreading across Skype | ZDNet

Security researchers from Avast have intercepted a currently spreading [Darkbot malware campaign](#), that's affecting millions of Skype users.

The malware spreads by messaging all of your contacts with a bogus "*new profile picture message*". It targets all the major Web browsers, and is also capable of distributing related malware such as Ransomware/LockScreen, as well as steal accounting data for major social networking services such as Facebook, Twitter, as well as related services such as GoDaddy, PayPal and Netflix.

What's particularly worth emphasizing on in regard to this malware variant, is that the messages used by the cybercriminals behind it have been localized to 31 different languages, with the malicious attackers relying on the GetLocaleInfo API function to ensure that they've properly geolocated the host.

Thanks to the rise of "[cultural diversity on demand](#)" services, literally each and every cybercriminal can embed [professionally translated messages](#) within their campaigns, potentially increasing the probability of having a potential victim click on these messages, and most importantly trust them, and their sender.

Users are advised to ensure that they're running the [latest version of their third-party software](#), [browser plugins](#), ensure that the URL they're about to click on hasn't already been [flagged as malicious](#), and take advantage of [application sandboxing techniques](#) to avoid direct exploitation of their host.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Local root escalation vulnerability in Mac OS X 10.4 and 10.5 discovered | ZDNet

Yesterday, an anonymous reader released details on [a local root escalation vulnerability in Mac OS x 10.4 and 10.5](#) , which

works by running a local AppleScript that would set the user ID to root through ARDAgent's default setuid root state. [Here's how it's done](#) :

"Half the Mac OS X boxes in the world (confirmed on Mac OS X 10.4 Tiger and 10.5 Leopard) can be rooted through AppleScript: **osascript -e 'tell app "ARDAgent" to do shell script "whoami" '**; Works for normal users and admins, provided the normal user wasn't switched to via fast user switching. Secure? I think not."

Find out how to fix it.

You've got several possible workarounds, you can remove the Apple Remote Desktop located in /System/Library/CoreServices/RemoteManagement/, or you can go through the [visual Workaround for the ARDAgent 'setuid root' problem](#) .

Moreover, the [AppleInsider speculates on the potential for abuse](#) :

The effects of malicious code run as root may range from deleting all the files on the Mac to more pernicious attacks such as changing system settings, and even setting up periodic tasks to perform them repeatedly. Not all Macs are vulnerable, however. If a user has turned on Remote Management in the Sharing pane of System Preferences under Mac OS X 10.5, or if a user has installed Apple Remote Desktop client under Mac OS X 10.4 or earlier and has activated this setting in the Sharing preferences, the exploit will not function. Mac OS X 10.5's Screen Sharing function has no effect on this vulnerability.

And even though the vulnerability can also be executed via a remote connection under specific circumstances based on the

configuration, physical security to prevent the unauthorized local access is as applicable as it's always been.

Legal concerns stop researchers from disrupting the Storm Worm botnet | ZDNet

What if security researchers were able to disrupt the leftovers of the Storm Worm botnet thanks to a flaw in its communication model allowing them to redirect infected hosts and eventually disinfect them, but fearing legal action have their hands tied?

At the [25th Chaos Communication Congress](#) , which took place in December, 2008, [German researchers](#) **Georg Wicherski** , **Tillmann Werner** , **Felix Leder** and **Mark Schlösser** , held a presentation ([Stormfucker: Owing the Storm Botnet](#)) demonstration their idea. The apparently working concept has a single flaw by itself - it operates in exactly the same fashion that a botnet master does when issuing updated malware binaries to the infected hosts, thereby violating computer abuse laws internationally.

Go through a Q&A with the researchers offering insights on the potential for distributed disinfection, and Storm Worm in general.

Q : How did you come up with the [Stormfucker](#) idea at the first place, and could you provide us with more details on the lack of server authentication when communicating to the infected clients that the Storm Worm botnet is vulnerable to?

Georg : On the 24c3 congress at the end of 2007, **Thorsten Holz** gave a presentation on disrupting Zhelatin's command and control infrastructure, involving a /16 network or 65536 nodes in other terms. This seemed both unfeasible to us and motivated to do better, we started analyzing Zhelatin binaries and eventually found out, that NAT'ed nodes don't require any authentication to be commanded at all.

They simply use a four-byte XOR challenge response for distinguishing between real command nodes and maybe accidentally connected nodes and that is it, as long as you implement the server protocol properly, you can command these nodes. Later it was brought to our attention that the small minority of non-NAT'ed nodes checks for a 64bit RSA signature, which is obviously trivial to crack.

Q : So basically, Stormfucker is capable of issuing potential disinfection commands to infected hosts meaning the botnet can be a thing from the past? What are the legal implications of saving the infected users from themselves here?

Georg : Stormfucker is able to send an update to a storm node that will then download an executable from a Stormfucker provided host and execute it. This executable would then be a Stormfucker executable that disinfects the computer and also aids in propagation of the update commands. Obviously, issuing a command to download and execute a file without the users' consent is against the law in many countries, let alone the then carried out further propagation of this command to other users.

Go through previous Storm Worm campaigns - [The Storm Worm would love to infect you](#) ; [Tracking down the Storm Worm malware](#) ; [Storm Worm's Independence Day campaign](#) ; [Storm Worm says the U.S have invaded Iran](#)

Q : The industry and the general public has never been comfortable with the idea of "white worms" or "ethical worms", and perhaps with a reason. Is this distributed disinfection method any different? Moreover, since there's never been a shortage of pragmatic solutions to a problem that's the main vehicle driving the cybercrime ecosystem, what would be the best way to put this pragmatic capabilities into action?

Georg : It is exactly like a white worm, the Stormfucker executable spreads from host-to-host in a distributed setup, however only targeting Zhelatin nodes -- other nodes will not see any extra traffic. Luckily some law enforcement agencies in some countries see the need to put an end to such menaces as Zhelatin and other botnets, maybe some of these people will push the button with proper legislation in the future. Rumor has it that it has happened in isolated cases before.

Q: What are your thoughts of a potential (free) opt-in service, where for instance, end users can request to be at least notified that they are part of Storm Worm's botnet or any other botnet in particular?

Georg: People who are so ignorant to execute an email attachment from an untrusted source would never sign up for such a service. A much better solution is taken by a local German ISP, NetCologne: they are allowed by their AUP to cut off users that are identified to be infected with malware and they have a Nepenthes based system to find such users. Being cut off from the Internet makes these ignorant people clean their computers pretty fast, so that they can browse the tubes again. Other ISPs should come up with similar solutions!

Q: Storm Worm's copycat Waledac (the same malware gang behind Storm) is currently spreading in the wild, would the same tactic work against it for instance, and how is Waledac's communication model any different than Storm Worm's original one?

Tillmann Werner : From the code perspective, waledac isn't storm's copycat, it's totally different, besides the fact that it also uses a p2p infrastructure. For instance, it communicates via encrypted XML messages over HTTP, thus it's immune to the sibyl attack. It does provide fast-flux DNS services similar to storm, but we would expect that from every serious malware these days, right? Some people think that there is the same group behind storm and waledac. Maybe, maybe not - who wants to know?

Felix Leder : Waledac is pretty new and the C&C structure not researched in-depth, yet. We are on it and may find something interesting. Currently we can only say that it is using "state-of-the-art" cryptography, which complicates things a bit but doesn't make it invulnerable. Instead of P2P, Waledac uses Fast-Flux networks. It is definitely possible to place controlled nodes in those networks. Whether those nodes can issue commands has to be investigated. So in short: The same tactics may work, but some more research has to be done.

The inside of Waledac is a lot different from Storm and similarities are hardly there. It is definitely a complete rewrite. The similarities (we have seen so far) are the use of open-source libraries in the malware, nodes that speak both storm and Waledac, and decentralized communication.

'Leaked Video of Casey Anthony CONFESSING to Lawyer!' scam spreading on Facebook | ZDNet

Researchers from Sophos have intercepted a [currently spreading Facebook likejacking scam](#).

Spamvertised as:

Click To See - She can't be re-tried, double jeopardy.. OJ all over again!

Users are enticed into clicking on a bogus video link from the mabwoo(dot)info domain. Upon clicking on the link users are asked to verify their age and click "Jaa" two times in order to play the video. Once they click on the button, the link will be automatically shared with all of their Facebook friends.

As always, the scammers are monetizing the campaign using paid surveys.

Users are advised to exercise extra caution when dealing with such scams.

'Leaked Video! Amy Winehouse on Crack hours before death' scam spreading on Facebook | ZDNet

Researchers from Sophos have spotted a [currently circulating Facebook scam](#), enticing users into clicking on a bogus Amy Winehouse-themed video link.

Spamvertised as:

Amy Winehouse is dead!!!Leaked Video!! Amy Winehouse On Crack hours before death. Amy Winehouse getting high on crack just hours before she died

Video leaked of amy winehouse's death!!! Warning: Graphical Content. Amy Winehouse OVERDOSE VIDEO LEAKED! - RIP AMY

The scammers are monetizing the campaign using paid surveys, earning a commission every time a user completes a survey.

Users are advised to be extra vigilant when interacting with link found on Facebook.

Latest version of Skype susceptible to malicious code injection flaw | ZDNet

According to a German security researcher, the latest version of Skype contains dangerous flaw, which could allow malicious injection of HTML/JavaScript code into a user's phone session.

Based on [an advisory](#) published on Wednesday, the researcher claims that:

An attacker could for example inject HTML/Javascript code. It has not been verified though, if it's possible to hijack cookies or to attack the underlying operating system. Attacker could give a try using extern .js files...

Skype's comments:

"We have had this reported to us by various media outlets and have confirmed that the person is mistaken, this is not a web window and while it does cause a phone number to be underlined, does nothing other than this," spokeswoman Brianna Reynaud wrote in an email.

However, the researcher said that the unsafe content is displayed when users view a booby-trapped profile, which works by inserting a JavaScript command or web address where a phone number is expected, since the entries in (home, office and mobile phone and city) are embedded via HTML.

Hat tip to [The Register](#) .

Lack of phishing attacks data sharing puts \$300M at stake annually | ZDNet

To share phishing URLs, or not to share? That's the rhetorical question, since sharing ultimately serves the final customer and ensures a lower average time for a phishing site to remain online. In a recently published research ([The consequence of non-cooperation in the fight against phishing](#)) Tyler Moore and Richard Clayton analyze the current state of delayed data sharing, and argue that the impact of non-cooperation among vendors is resulting in [an estimated \\$326 million annual loss](#) :

"The paper contains all the details, and gives all the figures to show that website lifetimes are extended by about 5 days when the take-down company is completely unaware of the site. On other occasions the company learns about the site some time after it is first detected by someone else; and this extends the lifetimes by an average of 2 days. Since extended lifetimes equate to more unsuspecting visitors handing over their credentials and having their bank accounts cleaned out, these delays can also be expressed in monetary terms. Using the rough and ready model [we developed last year](#) , we estimate that an extra \$326 million per annum is currently being put at risk by the lack of data sharing. This figure is from our analysis of just two companies' feeds, and there are several more such companies in this business.

Not surprisingly, our paper suggests that the take-down companies should be [sharing their data](#) , so that when they learn about websites attacking banks they don't have contracts with, they pass the details on to another company who can start to get the site removed."

Why wouldn't "take-down companies" be interested in sharing the data so that more customers get protected by visiting a phishing site that has already been shut down? Because the process of [taking down phishing sites](#) has been commercialized by vendors diversifying their [fraud protection and brand reputation services](#) a

long time ago. Such competition is in fact supposed to provide more value to the end users, since on their way to achieve better results than the competing company, the vendor will inevitably start taking down phishing sites more efficiently. However, as long as data is not shared so that a particular company can claim that it's taking down phishing sites faster than the other, the end users remain at risk.

In [a related research](#) published by Symantec in 2007, the company analyzed [the average online time for phishing sites](#) and argued that the take-down process is greatly affected based on the country the site is hosted in :

"Public phishing statistics often report the overall number of attacks hosted in a specific country, but this is not the only interesting detail: phishing attacks are more dangerous when they can "survive" online until the majority of potential victims open the phish email. Our analysis shows how ISPs in some countries are relatively slower than others to shut down attacks. For example, Taiwan's average shutdown time has been only 19 hours on 92 attacks, while in Australia the average for 98 attacks has been almost one week for a single shutdown. Other countries slow to respond include the USA and India. Countries identified as responding quickly include Germany, Netherlands, Japan, Estonia, Poland and Russia."

Non-profit community driven [projects such as Phishtank](#) and [StopBadware.org](#) are great examples of how this sharing mentality can protect most end users, so feeding these services with phishing/malware URLs in between ensuring that a phishing email never actually gets the chance to reach the inbox of an end user at the first place, is the way to go. Moreover, phishing emails are only part of the problem since [banker malware has gotten so efficient and sophisticated](#) , that I can easily argue that more money are at stake due to the increasing number of people infected with banker malware, compared to those interacting with phishing emails, since the banker malware remains active long after the phishing site has been shut down. Competitive practices must be balanced with social responsibility, which is where [sharing of data comes into play](#) .

Koobface worm joins the Twittersphere | ZDNet

Cybercriminals are experimenting with a new feature introduced in one of the [latest Koobface variants](#) - the ability of the worm to hijack the Twitter accounts of infected users and post tweets in an attempt to infect their followers.

According to researchers from TrendMicro, once the infected user attempts to log into Twitter, Koobface hijacks the session and posts a tweet on behalf of the user.

Would this novel feature allow the worm to spread even more efficiently? It largely depends on whether or not they'd remove the beta label from it, and go mainstream with the feature.

For the time being, the pre-defined set of messages include the following: *My home video :)* ; *michaeljackson' testament on youtube* and *Watch my new private video! LOL :)* . Interestingly, upon obtaining real-time statistics from their experimental Twitter campaign, the results show close to a hundred users that came to their bogus video serving ([W32.Koobface.A](#)) site through Twitter.

Compared to the automatic spreading of the worm across Facebook where the process of the [CAPTCHA challenge](#) recognition was [outsourced](#) , in Twitter's case the [lack of reliable use registration process](#) or any sort of CAPTCHA challenge, makes the [abuse of the micro-blogging service](#) incredibly easy to accomplish.

Has the worm's growth rate changed over the past month? According to recently released statistics from Kaspersky Labs, June was [the most active month for the Koobface gang](#) in terms of the number of samples generated -- 324 Koobface variants at the end of May 2009, to almost 1000 by the end of June 2009 -- a tactic used to increase the average time of their campaigns until they get intercepted. Earlier this year, [PandaLabs confirmed the growth rate](#) once again indicating the group's commitment.

For the time being, Koobface remains one of [the most active social networking worms](#) spreading across Facebook, Tagged,

Friendster, MySpace, MyYearBook, Fubar.com, Hi5 and Bebo since 2008, and despite the variety of new features, the worm continues relying on social engineering tactics in order to spread.

Koobface Facebook worm still spreading | ZDNet

Originally spreading [since July](#) , the Koobface worm remains active according to a recent [security alert issued by Websense](#) :

"The email reveals that infected user accounts are being used to post messages to Facebook friends lists. The content was an enticing message with a link that used a Facebook open redirector. When recipients click the link, they are automatically redirected multiple times, finally reaching a site masquerading as YouTube that serves a malicious Trojan downloader."

Koobface continues relying primarily on [already compromised Facebook accounts](#) as the foundation for its social engineering campaigns, the passwords to which the malware campaigners obtain through a changing [set of tactics](#) . How is Facebook responding to the persistent abuse of its services, and how are the tactics of the campaigners going to evolve in the long term?

The latest campaign is taking advantage of a legitimate hosting provider in the face of Geocities as a main redirection point, but what's particularly interesting about it is the fact that the malware dropper attempts to download more malware turning an infected host into a proxy relaying spam from another legitimate site - namely the American International Baseball Club in Vienna ([aibcvienna.org](#)), whose site seems to have been compromised. It's also worth pointing out that compared to other [malware campaigns abusing social networking sites](#) , the campaigns targeting Facebook and MySpace users rarely take advantage of bogus accounts, but rely on legitimate ones in only so that the campaign can scale while abusing the trust between the friends.

Social engineering and the fact the average social networking site user is still living in a "do not visit links sent from unknown people" and "do not visit unknown and potentially harmful sites" world, largely ignoring the fact that compromised legitimate sites and infected social networking profiles undermine these security tips, is

what malware campaigners try to excel at, but how come? [Site specific vulnerabilities](#) can indeed cause a lot of damage in a very short time frame, but the entire campaign will disappear as quickly as it appeared once the vulnerability gets fixed. Consequently, by applying the marginal thinking used by spammers sending out a million spam messages and profiting even if two people buy from them, reaching the end user next to targeting the site exclusively in order to remain beneath the radar for a bit longer, remains the (pragmatic) tactic of choice.

Facebook has been keeping track of the ongoing developments on the malware front, and has been adapting to the situation throughout the year. From [warning users on the potential maliciousness](#) of an ongoing link, to the recent [CAPTCHA challenge for grey links](#) aiming to slow down the spreading process of any campaign, these features are only the tip of the iceberg when fighting social networking malware campaigns. The rest is awareness in a trusted environment where everyone's identity can be compromised and abused.

Koobface botnet enters the Xmas season | ZDNet

The [Koobface botnet](#) , one of the most efficient social engineering driven botnets, is [entering the Xmas season with a newly introduced template](#) spoofing a YouTube video page, in between enticing the visitor into installing a bogus Adobe Flash Player Update ([New Koobface campaign spoofs Adobe's Flash updater](#)), which remains one of the most [popular social engineering tactics](#) used by the botnet masters.

What is the Koobface gang up to? Would they continue sticking to their true nature and rely on social engineering tactics, or would they start using active exploitation tactics such as client-side exploits?

Let's discuss some of the new developments introduced on the Koobface front over the past week, and try to answer these questions.

Experimenting with client-side exploits - last week, for the first time ever, the [Koobface botnet started serving client-side exploits](#) by embedding two iFrames on the hundreds of thousands of Koobface-infected hosts, for a period of several hours. Despite its [reliance](#) on outdated exploits [used by the](#) web malware [exploitation kit](#) in question, this does not automatically mean that their "infection optimization" strategy would go in vain taking into consideration the fact that a huge percentage of [users/enterprises continue failing](#) to properly manage their ["software inventory"](#) . Whether the gang would re-introduce the use of client-side exploits ([drive-by download](#)) remains yet to be seen, however, this move directly contradicts with the infection model of the botnet, which so far has been exclusively using social engineering tactics.

Constant diversification of legitimate services to abuse - in order to add additional layers of legitimacy, and increase its chances of bypassing reputation-based scanning mechanisms, the Koobface botnet is continue to put efforts into creating a self-sufficient botnet platform that's relying on the abuse of legitimate services only. Case

in point - a user [clicking on a bit.ly link generated by the Koobface botnet](#) , will get forwarded to the automatically generated **Blogspot** account registered with the help of an already infected with Koobface victim, which will then use a legitimate compromised site to finally load the Xmas season themed template from a Koobface infected host. A similar redirection will take place if the user clicks on the [spamvertised Google News redirector](#) , or [Google Reader link pushed by the Koobface botnet](#) .

Intensifying abuse of Bit.ly, the service strikes back - yesterday, **Bit.ly** , one of the [most popular URL shortening services](#) , which is also the service of choice for the Koobface botnet as of recently, [has announced](#) its [intention to add additional layers of security](#) by cooperating with **Verisign** , **Sophos** , **WebSense** in detecting malicious content using the service. The move will successfully position bit.ly as the URL shortening service with security in mind, taking into consideration the lack of such publicly acknowledged features in competing services, however, the sooner they implement it, the better, since the Koobface botnet masters have found a pragmatic way to trick users relying on **bit.ly's** preview feature months ago - in order to return a legitimate and recent news item, the automatically generated Blogspot accounts syndicate the title of a recent news item from **Google News** . The click-through rate on a sampled Koobface-generated **bit.ly** link speaks for itself - over 500 clicks within a 24-hour period.

Skype propagation module in the works - Two weeks ago, [security vendors](#) have intercepted a new [Koobface variant](#) (W32/Koobfa-O), which revealed more details into the gang's intention of abusing the **Skype** accounts of already infected victims, by spamvertising Koobface-service links to their Skype contacts. Interestingly, the sample was also [collecting personal Skype data](#) (*HOME PAGE, ABOUT, PHONE_MOBILE, PHONE_OFFICE, PHONE_HOME, CITY, COUNTRY, BIRTHDAY, FULLNAME, PSTN_BALANCE etc.*) and sending it back to the botnet masters, in what appears to be the foundation for a targeted marketing campaign tailored to the market segments which they're able to identify based on the collected data.

Skype, with its millions of users is naturally a target for separate

[scareware campaigns](#) which have been detected while using the application recently.

All of these recent developments clearly indicate the gang's intention to remain in business, as well as to continue maintaining its leading position in the [scareware business model](#) by pushing new [scareware variants](#) on each and every visit of Koobface-infected host.

Have you ever experienced a Koobface infection? Were some of your friends unknowingly spamming you with Koobface links, and did you tip them on the fact that they're infected? Do you think that the social networks most affected by Koobface should take a more radical approach when dealing with Koobface-infected users for the sake of providing a better service to the entire user base? Or is it [the ISP's role](#) to tackle [the problem at its roots](#) ?

TalkBack.

Kaspersky's Malaysian site hacked by Turkish hacker | ZDNet

According to Zone-h.org, [Kaspersky's Malaysian site has been defaced by a Turkish hacker](#) during the weekend, through a

SQL injection, [leaving the following message](#) - *"hacked by m0sted And Amen Kaspersky Shop Hax0red No War Turkish Hacker Thanx to Terrorist Crew all team members "*.

"The official Malaysian Kaspersky Antivirus's website has been hacked yesterday by a Turkish cracker going by the handle of "m0sted". Along with it, the same cracker hacked also the official Kaspersky S.E.S. online shop and its several other subdomains. The attacker reported "patriotism" as the reason behind the attack and "SQL Injection" as the technical way the intrusion was performed.

Both websites has been home page defaced as well as several other secondary pages. The incident, though appearing a simple website defacement, might carry along big risks for end-users because from both the websites, evaluation copies of the Kaspersky Antivirus are distributed to the public. In theory, the attacker could have uploaded trojanized versions of the antivirus, infecting in this way the unaware users attempting a download from a trusted Kaspersky's file repository (remember the trojan in the Debian file repository?)."

Are users at risk due to the compromise? Not in this case, however, the attack is a wake up call which if not taken seriously enough could result in an ironic situation where a security vendor's site is infecting its visitors with malware. It [has happened before](#) , and [it will](#) definitely [happen again](#) .

This is not an isolated incident. According to [Zone-h's archive](#) , since 2000 there have been 36 web site defacements of international Kaspersky sites, with Kaspersky's French site getting hacked and re-hacked on an yearly basis. And while in none of the incidents there was any malicious software served, or a live exploit URL that could have been embedded into the legitimate site, there's an ongoing

trend related to web site defacements in regard to their interest in [monetizing the access they have to the vulnerable sites](#) , by injecting [malware URLs](#) , hosting [phishing pages](#) , and also, locally hosting [blackhat SEO junk pages](#) where they would eventually earn money through affiliate based networks.

In the time of blogging there's no indication of a malware attack at the site, and **kaspersky.com.my** remains offline, presumably in an attempt to audit the site for web application vulnerabilities before putting it back online.

Related posts :

[300 Lithuanian sites hacked by Russian hackers](#) [China detains web site defacer spreading earthquake rumors](#) [Phoenix Mars Lander's mission site hacked](#) [Pro-Serbian hacktivists attacking Albanian web sites](#) [Comcast's DNS records hijacked, redirect to hacked page](#) [Photobucket's DNS records hijacked by Turkish hacking group](#) [ICANN and IANA's domains hijacked by Turkish hacking group](#)

Kaspersky: 12 different vulnerabilities detected on every PC | ZDNet

Researchers from [Kaspersky have sampled their customer base](#), and found out that on average, every PC has 12 different vulnerabilities.

During the second quarter of 2011, the company saw 27,289,171 vulnerable applications and files detected on users' computers, and detected an average of 12 different vulnerabilities on each computer.

Here are the vulnerabilities discovered:

Adobe Reader / Acrobat SING "uniqueName" Buffer Overflow Vulnerability

Sun Java JDK / JRE / SDK Multiple Vulnerabilities

Adobe Flash Player SharedObject Type Confusion Vulnerability

Adobe Flash Player Multiple Vulnerabilities

Adobe Flash Player Multiple Vulnerabilities

Sun Java JDK / JRE / SDK Multiple Vulnerabilities

Adobe Flash Player / AIR AVM2 Instruction Sequence Handling Vulnerability

Adobe Flash Player Unspecified Memory Corruption Vulnerability

Adobe Shockwave Player Multiple Vulnerabilities

Adobe Flash Player Unspecified Cross-Site Scripting Vulnerability

The company contributes the decline in Windows vulnerabilities, to improvements in the automatic Windows update mechanism and the growing proportion of users who have Windows 7 installed on their PCs. Moreover, Kaspersky Labs emphasizes on the fact that seven of the Top 10 vulnerabilities are found in one product only — Adobe Flash Player, and that vulnerabilities from 2007-2008 remain in the Top 10, with seven of the ten vulnerabilities were discovered in 2011, and the other three in 2010.

See also

[Secunia: Average insecure program per PC rate remains high Study: 6 out of every 10 users run vulnerable Adobe Reader 56](#)

percent of enterprise users using vulnerable Adobe Reader plugins

With vulnerabilities found in Acrobat Reader and Adobe products clearly dominating the threatscape, end users and enterprise users should ensure that they are running the latest versions of their installed applications and browser plugins , at any time.

Java zero day vulnerability actively used in targeted attacks | ZDNet

Security researchers from [FireEye](#), [AlienVault](#), and [DeependResearch](#) have intercepted targeted malware attacks utilizing the latest Java zero day exploit. The vulnerability affects Java 7 (1.7) Update 0 to 6. It does not affect Java 6 and below.

Based on [related reports](#), researchers were able to reproduce the exploit on Windows 7 SP1 with Java 7 Update 6. There's also [a Metasploit module](#) available.

Upon successful exploitation, the campaign drops [MD5: 4a55bf1448262bf71707eef7fc168f7d](#) - detected by 28 out of 42 antivirus scanners as Gen:Trojan.Heur.FU.bqW@a4uT4@bb; Backdoor:Win32/Poison.E

Users are advised to consider browsing the Web, and interacting with emails in an [isolated environment](#), or to block Java in their Web browsers until Oracle ships a patch for the security flaw.

Although what we've got here is a clear indication of an ongoing malicious attack utilizing a zero day flaw, on the majority of occasions cybercriminals wouldn't necessarily rely on a zero day flaw in order to infect as many users as possible. Instead, they would stick to using outdated and [already patched vulnerabilities](#) taking into consideration [the fact](#) that [end and](#) corporate [users](#) aren't [patching their third-party software](#) and [browser plugins](#).

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Italian-language page at MSN redirects to Cool Exploit Kit, serves ransomware | ZDNet

Last week, security researchers from [AVG's Web Threat Research group](#) detected a malicious JavaScript on an Italian-language page at MSN, which was at the time redirecting to [the Cool Exploit Kit](#) , ultimately dropping ransomware on the affected hosts.

The high profile Web site infection, in terms of the huge traffic volume that was logically hijacked during the campaign, raises an important question--can you really trust those "Trusted Web Sites" that average and corporate users often think are secure by default? The truth is that you can't afford to "wait and see," and need to always assume the worst, for the sake of your data/host/network's CIA (Confidentiality, Integrity, Availability).

Throughout the years, cybercriminals have learned that it's easier and more efficient to inject malicious scripts on hundreds of thousands of Web pages, instead of targeting a few high profile Web sites. It's not that they don't want to. It's just more efficient and easy to utilize the "Long Tail" concept. Naturally, that entirely depends on the attackers in question.

For instance, this isn't the first time that pages within MSN's domain were serving malware to its visitors. Back in 2008, [MSN Norway fell victim to a malvertising campaign](#) , followed by a series of direct/indirect compromises of high trafficked Web sites throughout the entirety of 2009, affecting [FoxNews.com](#) , [Cleveland.com](#) , the [New York Times](#) , as well as [many other high profile Web sites](#) such as, [CNN](#) , [BBC](#) , [Washington Post](#) , [GameSpot](#) , [World Of Warcraft](#) , [Mashable](#) , [Chow.com](#) , [ITpro.co.uk](#) , [AndroidCommunity](#) , [Engadget](#) , and [Chip.de](#) , proving that no one is safe. And although the media's attention is constantly emphasizing on the emergence of targeted attacks and cyber espionage campaigns, noisy mass SQL injection campaigns and traffic acquisition tactics relying on malvertising, are definitely not a thing from the past.

AVG has notified Microsoft, and the malicious JavaScript has been removed.

Do you think the time has come for the industry to admit that there's no such thing as a trusted Web site, and that users should always assume the worst by default? Do you maintain a list of trusted Web site, and what makes you think they're trusted enough to be allowed to run active content?

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

IT expert executed in Iran | ZDNet

Following Pakistan's recently introduced "[Prevention of Electronic Crimes Ordinance 2008](#)" according to which potential cyberterrorists would face the death penalty, a neighboring country, Iran, [has recently executed an IT expert who confessed of being an Israeli spy](#) for at least three years. After being recruited by Mossad during a business trip, Ali Ashtari, a trusted supplier of electronic and military equipment for the Iranian government, was allowing Israeli intelligence agents to backdoor the equipment he would later on install in Iranian military and government centers.

"Behind their backs he allowed the software he bought to be subtly doctored by Israeli computer engineers before it was imported to Iran. Ashtari confessed: "Mossad's goal was to sell specialised computer equipment through me to Iranian intelligence organisations." Ashtari revealed how he communicated with his Israeli controllers: "I received a laptop with encrypted software for fast e-mail communication," he said. "They asked me to install bugging devices in the communications equipment I provided to my clients."

Once the physical security of the devices has been compromised, anything from remote control capabilities to scheduled malfunctioning through logic bombs could have been integrated within. [Despite the fact](#) that they wanted him to give a [portable satellite Internet device](#) to the Iranian government, it still remains unknown to what extent and what type of backdoored equipment he has already introduced on behalf of the foreign agents.

The concept of backdooring hardware is nothing new, take for instance such proof of concepts like the [Illinois Malicious Processors \(IMPs\)](#) allowing high level access to a system running the backdoored hardware. In fact, the potential for damage and espionage activities is so realistic, that in [a leaked FBI presentation entitled "Cisco Routers"](#) the agency assesses the risks posed by counterfeit Cisco routers somehow making it into the critical infrastructure network.

The weakest link? It's the subcontracting process.

Israeli Institute for National Security Studies compromised, serving Poison Ivy DIY malware | ZDNet

According to [security researchers from Websense](#), the web site of the Israeli Institute for National Security Studies (INSS) has been compromised, and is currently serving client-side exploits and malware to its visitors.

Upon visiting its web site, users are exposed to malicious iFrame redirects, ultimately serving the client-side exploit from the following IP - **194.183.224.73**.

The campaign ultimately exploits the well known Java vulnerability [CVE-2012-0507](#), in an attempt to serve a copy of the Poison Ivy RAT (remote access tool).

Detection rate:

svchost.exe

[MD5: 52aa791a524b61b129344f10b4712f52](#)

Detected by 29 out of 42 antivirus vendors as Backdoor.Win32.Poison.dizt.

Upon execution, the sample connects to a Dynamic DNS command and control address at: **ids.ns01.us**

Websense has notified the affected web site, but so far hasn't heard back from its web master. According to the company, the attack appears to be isolated incident, and not part of a massive client-side exploits serving campaign currently circulating in the wild.

Is Mozilla's Firefox 'click-to-play' feature a sound response to drive-by malware attacks? | ZDNet

According to a [blog post by Mozilla's software engineer Jared Wein](#), Mozilla plans to introduce 'click-to-play' feature in upcoming versions of their flagship Firefox browser.

The feature -- available to [NoScript](#) users for years -- aims to prevent the systematic exploitation of browser plugin based client-side exploitation campaigns, by allowing end users to choose whether they would want to active content to load in the first place.

A logical question emerges - is this a sound response to preventing the currently ubiquitous exploitation of client-side vulnerabilities on end and corporate PCs, [especially in times](#) when [the average user](#) is running a number of [remotely exploitable](#) third-party applications and [browser plugins](#)?

Not necessarily. How come? Pretty simple.

Basically, what Mozilla's 'click-to-play' feature really does, is slowing down the systematic exploitation of client-side vulnerabilities, not preventing it. On the majority of occasions, drive-by malware attacks are launched with [a social engineering element](#) in an attempt to increase the probability for a successful infection.

Cybercriminals entice end users and provoke end user interaction by promising something in return for clicking on the malicious link found found in spamvertised emails. If the end user originally clicked on a link promising him a video clip, access to personal data, notification, or verification email, Firefox's 'click-to-play' feature will only slow down the exploitation process, as the end user will eventually enable the showing of active content in an attempt to access the promised content.

Moreover, as we've seen in the past, cybercriminals are masters of visual social engineering, successfully impersonating well known brands, consumer products, and product features, such as for

instance [Firefox's security alert](#), and [SafeBrowsing initiative's warning page](#). It would take long before they start mimicking Mozilla's 'click-to-play' feature, offering additional advice to users for enabling it in order to view the promised content.

What do you think? Is Mozilla's 'click-to-play' feature a sound response to preventing drive-by malware attacks? Or are social engineering elements embedded in these campaigns undermining the usability of Mozilla's feature?

Talkback.

Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites | ZDNet

Approximately 24 hours ago, the [Iranian opposition](#) coordinated an ongoing cyber attack that has successfully managed to disrupt access to [major pro-Ahmadinejad Iranian web sites](#), including the President's homepage which continues returning a "*The maximum number of user reached, Server is too busy, please try again later...*" message.

Through a combination of DIY (do it yourself) denial of service attack tools (DDoS), multiple iFrame loading scripts, public web page "refresher" tool, and a much more effective PHP script, the participants have already prompted some of the major Iranian outlets to switch to "lite" versions of their sites in an attempt to mitigate the attack.

Let's assess this very latest example of people's information warfare concept, find out which sites remain affected, and discuss the attack tools used:

The campaign appears to have been organized through Twitter, which despite public reports that the site has been banned in Iran, appears to be still accessible through a persistent supply of proxy servers on behalf of the opposition.

Moreover, the ongoing distributed denial of service attacks, are using techniques which greatly resemble those used in [last year's Russia vs Georgia cyber attack](#), and the ones [Chinese hacktivists used back in 2008 in order to temporarily shut down CNN](#), with a single exception - there's no indication of a botnet involvement in the present attack.

Instead, the attack relies on the so called [people's information warfare concept](#), which is the self-mobilization of individuals, or their recruitment based on political/nationalistic sentiments by a third-party, for conducting various hacktivism activities such as web site defacements, or launching distributed denial of service attacks.

The following are some of the sites that are currently under attack, remain totally unresponsive, or return "server is too busy" error messages:

Ahmadinejad.ir - Mahmoud Ahmadinejad's Official Blog - under attack

Leader.ir - Office of the Supreme Leader, Sayyid Ali Khamenei - under attack

President.ir - Presidency of The Islamic Republic - under attack

Farsnnews.com - Fars News Agency - under attack

Irib.ir - Islamic Republic of Iran Broadcasting - under attack

Kayhannews.ir - News Portal - "Service Unavailable"

Irna.ir - Islamic Republic News Agency - "service unavailable"

Mfa.gov.ir - Ministry of foreign affairs , Islamic Republic of Iran - under attack

Moi.ir - Ministry of Interior - under attack

Police.ir - National Police - under attack

Justice.ir - Ministry of Justice - under attack

Presstv.ir - Iranian Press TV - "server is too busy"

Chatter from the hacktivists' trenches send over Twitter, or web forums during the past 24 hours:

- "Overload Iran's propaganda websites--we can do it together!" -
"we can suspend IRIB propaganda! just click & keep it refreshing!" -
"Take part in disabling the iranian propeganda leave on as long as possible" - "Our efforts are working!!! RT @NewIRAN: Leader.ir; President.ir; FarsNews.com all now appear to be down" - "Iran needs your help. Help us flood Iran Govt sites khamenei.ir is one of our targets. Go to PageReboot.com and set @ 2 secs" - "we are currently flooding Iran Government websites - we have successfully taken down numerous sites already" - "Great news! PressTV.ir has been shut down thanks to our efforts!" - "IRIB, RESALAT, Kayhan, FarsNews, President.ir, and Leader.ir all brought down. Please help keep them down." - "president.ir is down!!!" - "SPREAD: tool for denial of service web attack. run on president.ir and irib.ir" - "I'm reaping at 200kb/sec baby." - "sweeeeeet, Farsnews is finally down! keep it up guys. I have 5 browsers open using Page Reboot." - "Let's continue the attack. They have a very efficient server compared to

other sites, but we successfully killed it many times already. Try to reload your application." - "It's down again. I can't view it from NZ. Keep at it people." - "I'm going to set up a massive solo attack on Resalat using 8 virtual machines on 8 CPUs while I go to bed. I understand it'll be hard to make it go down but I'm going to try." - "done. I am also using couple of virtual M. Lets see if we can bring it down." - "HAHAHAHAHAHAHAHAHAHA!!!! RESALAT DOWN!!!!!!!!!!!! THAT WAS F*CKING BRUTAL!!!!"

Among the first web-based denial of service attack used, is a tool called "Page Rebooter" which is basically allowing everyone to set an interval for refreshing a particular page, in this case it's 1 second. Pre-defined links to the targeted sites were then distributed across Twitter and the Web, through messages link the following :

"Please spread word about a cyber effort to exert pressure on the paramilitary in Iran. They have launched denial of service attacks on US websites that are run by live bloggers feeding us up to the minute information about what is going on in Iran on the ground. To fight back, open these two URLs in as many tabs/windows as possible and simply leave your computer running overnight! We must show solidarity with them in their quest for freedom! The 2nd link targets PressTV, the mouthpiece of Ahmadinejad and Khamenei."

The second stage of the campaign consisted in the distribution of a multiple iFrame loading script which was automatically refreshing **farsnews.com** ; **irna.ir** and **rajanews.com** , the results of which you can see in the attached screenshot. The script has since changed its location and is advertised under a new domain.

[Next](#) -->

The third stage included a combined attack, this time including DIY (do-it-yourself) denial of service tools (DDoS), which despite their primitive nature are indeed causing server overload for their targets. Each of the tools is distributed with a simple manual, including links to large images at the targeted web sites, one which the software using proxies will attempt to obtain automatically.

Go through related hacktivism posts: [Chinese hackers deface the Russian Consulate in Shanghai](#) ; [Georgia President's web site under DDoS attack from Russian hackers](#) ; [Thousands of Israeli web sites](#)

[under attack](#) ; [Pro-Serbian hacktivists attacking Albanian web sites](#) ; [Hundreds of Dutch web sites hacked by Islamic hackers](#) ; [300 Lithuanian sites hacked by Russian hackers](#) ; [Chinese hackers deface the Russian Consulate in Shanghai](#) ; [China detains web site defacer spreading earthquake rumors](#)

The tools themselves, **BWRaeper.exe** (detected as [Worm.AutoIt.AA](#)); **PingFlooder.exe** (flagged as [banker malware](#)); **Server_Attack_By-_C-4.exe** ([Riskware.ServerAttack.F](#)) and **SupportIran.php** , have already been picked up by antivirus vendors.

The following are the instructions found in the **StopAhmadinejadOnline** package, consisting of **BWRaeper.exe** and **PingFlooder.exe** :

"New hacking/DoS attack tool. Please learn and use: This is an online war 1. Please download 2. Extract it into a folder on your desktop and click on BWRaeper 3. Then click on Raep That's all.

FarsNews, AN's website, KHamenei's Website, IRIB and many other sites can be brought down with this technique. This is an online war. Don't let them win. They filter information, we will too. There's more of us. EDIT: Please add the following URLs to your list of URLs after you've completed the steps above. To do this, open the file "urls.txt" and paste the following line in it. Once you've added this URL, Run BWRaeper again

irna.ir/Images/uilimages.gif resalat-news.com/Pic/6729000.jpg
resalat-news.com/image/Heder.jpg resalat-news.com/Pic/6729.gif
resalat-news.com/Pic/6729011.jpg resalat-news.com/Pic/6729021.jpg"

The manual within **Server_Attack_By-_C-4.exe** entices users to participate in the attack, in the following way:

"I also found another DOS file to attack. just another option. 1. dl this zip file from here and unzip it on ur desktop: 2. take IP address of IR sites(Farsnews.com, irna.ir, president.ir, rajanews.com) from here: http://www.selfseo.com/find_ip_address_of_a_website.php 3. insert the IP address in "Server Address" section and press Attack. 4. let it run and it'll attack all of their servers"

The last tool is a basic PHP script targeting those running a server that supports PHP in order to use it - *"Want to help DDoS attack Iran gov't? Have a server that runs PHP? Use this script!"*.

SupportIran.php has also been released as an improved version to the multiple iFrame loader, and is currently used in the attack as well, having the following sites pre-defined to attack simultaneously - **khamenei.ir ; presstv.ir ; irna.ir ; president.ir ; mfa.gov.ir ; moi.ir ; police.ir ; justice.ir; live.tribe.ir** .

There have already been speculations that the magnitude of these local attacks -- [Iranian users targeting Iranian web sites](#) -- is contributing to the "[strange changes in Iranian traffic transit](#) " reported during the last couple of days.

The attacks are ongoing, updates will be posted as soon as they emerge.

An update to the [ongoing DDoS attacks](#) has been posted.

iPhone's anti-phishing protection offers inconsistent results | ZDNet

Apple's iPhone OS 3.1 update includes a new [fraud warning feature](#) which is at least theoretically, supposed to warn users when visiting fraudulent websites in Safari Mobile.

However, due to a flawed implementation in the update mechanism, the feature -- enabled by default -- is offering inconsistent results based on the tests performed by [security company Intego](#), and security researcher [Michael Sutton from Zscaler](#), whose posts basically state that "*it simply doesn't work*".

Here's how they tested the feature:

The tests were conducted by pulling data of [valid phishing sites from the Phishtank](#), and attempting to visit these sites in Safari and Safari Mobile, which resulted in their successful detection in Safari, but didn't trigger a warning when visiting the same sites on the iPhone's Safari Mobile.

Go through related posts: [Snow Leopard's malware protection only scans for two Trojans](#); [Snow Leopard ships with vulnerable Flash Player](#)

The cause for these inconsistent results appears to be a flawed update mechanism, lacking any transparent way of communicating when was the last time an update took place, as well as a built-in "valid time" interval indicating that an outdated anti-phishing database is in use.

A few minutes ago, [Intego posted an update](#) to the original post in regard to the varying results:

We've had a number of people test this, and some people get warnings for sites that others can load just fine. We've tried isolating locations, iPhone/iPod touch models, and whether they are connecting over a cell network or via wifi, but all we've come up with is that sometimes it works and sometimes it doesn't. This is clearly

more dangerous than no protection at all, because if users think they are protected, they are less careful about which links they click.

The company makes a good point, however, there are several more issues to consider. For instance, in comparison to Safari Mobile's fraud warning feature and its lack of transparency into the update mechanism, a commercial [iPhone app](#) called [Site Check](#) is utilizing the SafeBrowsing API in between offering a transparent way of knowing the last time a database update took place, with the option to manually pull one at any particular moment in time. This very same practice should also be implemented in the fraud warning feature.

Moreover, an assessment of the [fraud warning feature](#) at Macworld, points out that compared to Google Classic run on Safari Mobile, Google Mobile isn't showing [potentially harmful and fraudulent web sites](#) , once again leaving users with the impression that they're surfing the web and clicking on links under the umbrella of the SafeBrowsing initiative.

Transparent processes and [customerization](#) always translate into improved customer satisfaction, in this particular case, improved security as well.

iPhone 5 themed emails serve Windows malware | ZDNet

Researchers from Sophos have intercepted a [currently spamvertised malware campaign](#), attempting to socially engineer users into clicking on a malicious link.

Event-based social engineering campaigns aim to capitalize on current or upcoming events for malicious purposes. In this case, Apple's upcoming iPhone 5 release seems to have attracted the attention of cybercriminals.

The malware is detected as Mal/Zapchas-A.

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Imagery courtesy of [PCMAbram](#).

Internet Explorer 9 outperforms competing browsers in malware blocking test | ZDNet

According to a [newly released research by NSS Labs](#), Microsoft's Internet Explorer 9 greatly outperforms competing browsers in a test against socially-engineered malware. Based on an active testing against 615 malicious URLs for 19 days, both Internet Explorer 9 and Internet Explorer 8 topped the comparative chart.

Here are the findings:

Windows Internet Explorer 9 - IE9 caught an exceptional 92% of the live threats **Windows Internet Explorer 8** - caught 90% of the live threats **Apple Safari 5** - caught 13% of the live threats **Google Chrome 10** - caught 13% of the live threats **Mozilla Firefox 4** - caught 13% of the live threats **Opera 11** - caught 5% of the live threats

More details:

With SmartScreen enabled and Application Reputation disabled, IE9 achieved a unique URL blocking score of 89% and over-time protection rating of 92%. Enabling Application Reputation on top of SmartScreen increased the unique URL block rate of Internet Explorer 9 by 11% (to 100%) at zero hour as well as the over-time protection by 8% (to 100%). Internet Explorer 9 was by far the best at protecting against socially-engineered malware, even before App Rep's protection is layered on top of SmartScreen.

Why are NSS Labs' findings not necessarily accurate?

This isn't the first time I've criticized research published by NSS Labs, and definitely not the last. Not only is the research ignoring the existence of client-side vulnerabilities, its methodology is fundamentally flawed taking into consideration the limited number of URLs the browsers are tested against, combined with lack of testing of the additional protection features offered by the competing browsers and the related security add-ons.

See:

[Study: IE8's SmartScreen leads in malware protection IE8 outperforms competing browsers in malware protection -- again](#)

An excerpt:

By excluding client-side vulnerabilities, the study isn't assessing IE8's DEP/NX memory protection, as well as omitting ClickJacking defenses and IE8's XSS filter, once pointed out as a less sophisticated alternative to the Firefox-friendly NoScript.

Socially engineered malware is not the benchmark for a comprehensive assessment of a browser's malware block rate. It's a realistic assessment of the current and emerging threatscape combined with comprehensive testing of all of the browser's currently available security mechanisms, a testing methodology which I think is not present in the study.

What do you think? Isn't the fact that client-side vulnerabilities are excluded, undermining the benchmarking methodology used? What about the lack of measurement of vulnerable and outdated browser plugins which could lead to a successful exploitation through a web based malware exploitation kit?

Talkback.

Image courtesy of NSS Labs.

International Kaspersky sites susceptible to SQL injection attacks | ZDNet

According to a security group going under the name of [TeamElite](#) , the international sites of Kaspersky Iran (**kasperskylabs.ir**), Taiwan (**web.kaspersky.com.tw**) and South Korea (**kasperskymall.co.kr**) are [susceptible to SQL injection attacks](#) , allowing the injection of malicious iFrames and potentially assisting malicious attackers into obtaining sensitive data from the web sites in question.

The group's analysis comes shortly after the series of posts by a Romanian group of serial pen-testers of security vendors, which discovered similar flaws in the web sites of [F-Secure](#) , [Symantec](#) , [BitDiffender](#) , and [Kaspersky USA](#) .

Let's start from the basics. PR contingency planning in the spirit of total denial is perhaps the worst thing a vendor can do in this case. Despite the fact that these are reseller web sites and are managed by local companies, they still have the license to harness the power of the brand of an information security company, and therefore not demonstrating basic security awareness by taking care of trivial web application vulnerabilities on these sites, can undermine the brand's integrity and what it stands for at the first place.

From a pragmatic perspective, the licensing company can either exercise pen-testing authority over the locally managed web sites, keep an eye on them through [community service warning systems](#) , or introduce obligatory pen-testing before a license is obtained.

Both groups have been notifying the affected vendors according to their posts.

Intel proactively fixes security flaws in its chips | ZDNet

Despite the skepticism surrounding Kris Kaspersky's upcoming ["Remote code execution through Intel CPU bugs"](#)

presentation to be held at this year's Hack in the Box con, it appears that he's been on the right track, as Intel has proactively taken care of the problem by [fixing two of the critical flaws according to Kaspersky](#) :

"On Friday, Kaspersky told Computerworld that he has been communicating with Intel about the flaws for nearly a month and the company has told him that it fixed the two critical flaws he brought to Intel's attention. Both of the flaws -- one in the cache controller and one in the Arithmetic logic unit -- could be used by a remote attacker to execute arbitrary code, according to Kaspersky."

And whereas he's been asked not to release proof of concept code at the conference due to the potential implications given Intel's leading market share, and the fact that the flaw is OS independent, he'll be releasing technical details on the vulnerability. Was Intel caught off guard at the first place?

Depends on the perspective. Intel has been actively investing in R&D of security technologies to make their chips more

secure. An example of such a successful effort is [Intel's Trusted Execution Technology](#), already introduced in several of their chip families :

"Intel® Trusted Execution Technology for safer computing, formerly code named LaGrande Technology, is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. Intel Trusted Execution Technology provides hardware-based mechanisms that help protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the client PC. It does this by enabling an environment where applications can run within their own space,

protected from all other software on the system. These capabilities provide the protection mechanisms, rooted in hardware, that are necessary to provide trust in the application's execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform"

The question based on Kaspersky's modest details ahead of the presentation is, whether or not he'll be demonstrating [direct Java bytecode execution](#) , and which chip families is he going to target. One thing's for sure, when a vendor is proactively fixing vulnerabilities you were speculating about based on off the record discussions with you, you knew what you were looking for.

Inside the botnets that never make the news - a gallery | ZDNet

If you ever wanted to take an inside view of targeted-botnets primarily run by novice cybercriminals sometimes utilizing outdated, but very effective methods - this [ZDNet photo gallery](#) is for you.

It offers an inside view of those "beneath the radar" botnets that never make the news. The images have been collected throughout the past year by using open source intelligence, namely, by either joining the command and control IRC channel upon infection, or monitoring ongoing communications between the botnet masters.

Why are [small botnets](#) so important anyway, and [shouldn't we keep](#) an eye on the [big ones](#) such as [Conficker](#) , [Torpig](#) or the rest of [the eye-popping](#) ones? Smaller botnets are usually underestimated ones, however, they're perfectly suitable for targeted attacks such as the recently exposed [GhostNet espionage network](#) . Moreover, despite the massive botnets run by sophisticated cybercriminals, evidence in the past ([Storm Worm Hosting Pharmaceutical Scams](#) ; [Money Mule Recruiters use ASProx's Fast Fluxing Services](#) ; [Inside the Srizbi Botnet Business Model](#)) clearly indicates that they're partitioning the botnets and reselling pieces of the pie to other cybercriminals, which would then simply remove the original malware and introduce one of their own.

These small botnets are also exclusively used for some of the sophisticated managed spam services currently offered on the underground marketplace. For instance, the [managed spamming service](#) exclusively profiled by Zero Day last year, was using only 5000 infected hosts for the purpose of sending 1 million spam messages. Another variation of it was offering only 1672 infected hosts, and was still capable of [spamming 3215 emails per minute](#) .

For the time being, the massive botnets we're used to seeing aren't going away, but in the long term the cybercriminals behind them could easily start splitting/partitioning them for operational security, and in order to avoid [potential mass hijacking](#) from

[competing cybecriminals](#) or security researchers - the malicious economies of scale that cybercriminals achieve by standardizing the exploitation process [also means](#) that their [crimeware botnets](#) are [vulnerable to](#) the logical [monocultural insecurities](#) .

What do you think?

Inside India's CAPTCHA solving economy | ZDNet

No [CAPTCHA can survive](#) a human that's receiving financial incentives for solving it, and with an army of low-waged

human CAPTCHA solvers officially in the business of "data processing" while earning a mere \$2 for solving a thousand CAPTCHA's, I'm already starting to see evidence of consolidation between India's major [CAPTCHA solving companies](#) . The consolidation logically leading to increased bargaining power, is resulting in an international franchising model recruiting data processing workers empowered with do-it-yourself [CAPTCHA syndication web based kits, API keys, and thousands of proxies](#) to make their work easier, and the process more efficient.

Let's analyze the shady data processing economy of India, discuss exclusive photos of Indian workers breaking MySpace and Google CAPTCHAs, and take a tour inside the web applications of several Bangladesh based franchises, whose team of almost 1,000 international workers is actively soliciting deals for breaking Craigslist, [Gmail, Yahoo](#) , MySpace, YouTube and Facebook's CAPTCHA, promising to deliver 250k solved CAPTCHAs per day on a "\$2 for a 1000 solved CAPTCHAs" rate.

One of the services in question is the India based **decaptcher.com** , which will allow you to retrieve its API once you put

money in their PayPal account :

"Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services. Solve CAPTCHAs with the help of this portal, increase your business efficiency now! Follow these steps:

1. Register
2. Contact us at admin@decaptcher.com to put money to your account via PayPal and retrieve API
3. Login to check your balance

You pay for correctly recognized CAPTCHAs only"

The service is among the countless number of franchises operated by several of India's large data processing companies,

making it harder, but not necessarily impossible to establish connection between them. At the beginning, mom and pop CAPTCHA services seeking to expand start participating in the franchise business model offered by the big companies that are no longer capable of executing the projects on their own, and so in a win-win-win situation for the big company, the franchise, and the customers, India's CAPTCHA solving economy is booming.

Moreover, the investments made in purchasing the PCs, the web proxies, the training and education of the staff by providing them with tips for increasing their CAPTCHA solving productivity, as well as the sophistication of the web based applications aiming to empower non-technical users, clearly explain why India remains the market leader in CAPTCHA solving, with thousands of legitimate data processing workers converted to CAPTCHA solvers.

From a legal perspective, the creativity of the marketers behind these services is simply amazing. Here come the socially

oriented " CAPTCHA solving service aiming to serve the visually impaired, the fake academic looking for technical know-how in breaking Gmail's CAPTCHA for his research project, to the companies interested in helping you increase your business efficiency by allowing you to automatically abuse a particular service and reach more potential customers.

Data processing as a mentality is visible in all the applications a human CAPTCHA solver is using. Basically, there's no indication which service's authentication model they're currently abusing, CAPTCHA breaking is replaced with CAPTCHA solving making it look like it's a some sort of a challenge that they have to solve.

Recruitment of the people that would be later tested for whether on not they quality for the job by exposing them to

CAPTCHAs from different services, and a timer running in the background, is mainly done through advertisements like the following :

* easy work * no learning needed * no investment needed * weekly payout * work from home * work when you want * flexible working hours * highest rates in the industry

How serious is the CAPTCHA solving business in India? The following Indian advertisements of their CAPTCHA services clearly speak for themselves - business is good and they are in fact competing for projects :

24/7 support still like. We have 30 pc 90 worker & we have 300 captcha team. Your any captcha project we done quickly. We have high experience captcha worker

Sir, We have 10 systems with good typing skill workers. We can easily do 25k per day

I have 40 PCs and 55 Persons working in my office for data entry work. As 1 person can do 800 captcha entry per hour. We can deliver you good quantity with quality

Hello Sir, I will kindly introduce myself.. This is shivakumar.. we have a team to type capcthas 24/7 and we can type more than 200k captchas per day

WE ARE PROFESSIONAL CAPCHA ENTRY OPEATORS AND WE CAN DO EVEN 25000 ENTRIES PER DAY AS MY COMPANY IS A 25 SEATER FIRM SPEALISED IN DATA ENTRY

Our Team is very much interested in your project and we could easily handle more than 50,000 captcha entries per day

We having more then 10 teams,we are operating 24/7 data entry works and delivering 700k/day captchas daily

I have a team of 7 people, willing to do captchas at \$2 per 1000 entries. Please consider my bid. We can definitely provide 50K captchas per day

I have 40 PCs and 55 Persons working in my office for data entry work. As 1 person can do 800 captcha entry per hour. We can deliver you good quantity with quality

My team is equipped to offer the services. 20 person team, T1 business speed internet with an on hand technical staff. We are able to start right away

Dear Sir I am an expert in account creation, will provide you the accounts as per your requirements.I ensure the guaranteed satisfaction always. I charge only \$40/1000

captcha typing teams for 24/7 ready. Rate \$1.25 for 1K, up to 100K captchas per day

1\$ per 1K of entries, and ready to produce 50 K entries per day.

Kindly look forward procedures to provide the chance to us

My rate \$4.00 per 1k My team can work 24/7. They are jobless now

\$3 per 1000 image entry, Ready start. 24/7 service like also. We have 30 pc 90 worker & 39 big captcha team so your any target we solve

Dear Sir, We have quoted 50 \$ per 50000 entries., Kindly look forward procedures to provide a chance to work with you

700,00 broken CAPTCHA per day would be surreal, unless of course we take into consideration the consolidation and

franchising among the smaller groups of CAPTCHA "experts". Another advertisement from a relatively bigger company is forwarding the responsibility for downtime to MySpace, which according to them is often down so that they cannot do their job as efficiently as their infrastructure allows them to :

"This is long term project Rate is 1.50\$ / 1000 entry. We need teams that can do 24/7 captcha entry. We are looking for individual teams to provide 10,000 to 200,000 entries per day per team. We require 90% accuracy and avg entry time less than 10 seconds. Real time stats. 3x a week pay via paypal only. \$1.50/1k or best bid. Outsourcing is allowed. Teams that can provide 24 hour service will be preferred. Don't waste your and our time!!

Our captcha system is very complex and complicated. It is built to process up to one million captchas per day.

We have several big teams and hundreds of active agents solving captchas, all at one time, especially during daytime in India. The backend of this project involves over 45 powerful, expensive servers communicating with the MySpace site to pull the captchas and then queue them up on this site, and then process the results to push back to MySpace all within 20 seconds per captcha.

We run into many slowdowns. The most common bottleneck is that MySpace itself is often bogged down, slow and error prone, which then makes it very difficult for our servers to pull captchas

quickly. Also much of the work on our servers is handled internationally, so the Internet connections have lag time.

Usually when the server takes a long time to show a new captcha, it is waiting for our other servers to pull

another captcha. Sometimes 100 or more agents are waiting at the same time, so the queue only goes to one agent at a time. We recommend you try to work during afternoon and evening USA times (night time in India).

We are constantly trying to improve the speed of our site. We also continue to grow with expanding captcha teams and agents. Scaling our site is time consuming and expensive so implementation is not an immediate process."

Consider going through several other India based CAPTCHA solving companies, targeting multiple different CAPTCHAs, but also, clearly emphasizing on Google's while working on a Google related project :

The bottom line - is text based CAPTCHA dead? It's definitely in pain thanks to evil marketers recruiting low-waged Indian data processing workers, who according to some of the statistics obtained, earn over ten times more while solving CAPTCHAs, than through their legitimate data processing jobs.

Inside BBC's Chimera botnet | ZDNet

Earlier this month, the controversial [BBC purchase of a botnet](#) and modifying the infected hosts in the name of "public interest" sparked a lot of debate on the pros and cons of their action. [Condemned](#) by certain [security vendors](#) , and naturally, at least from guerrilla PR perspective, [applauded and encouraged as a awareness raising tactic](#) by others, the discussion shifted from technical to moral and legal debate, leaving a single question unanswered - what is the name of the botnet that the BBC rented and what's so special about it?

Until now. Let's take a peek inside the BBC "Chimera Botnet" offered for rent by a Russian Cybercrime-as-a-service (CaaS) vendor.

While watching the BBC's Click programme, I was particularly surprised by the fact that the botnet's backend appeared to be a brand new one, presumably released in recent weeks. Digging a little deeper that proved to be the case with the managed botnet vendor starting to pitch it publicly at the beginning of the year. Moreover, being involved in profiling, obtaining and analyzing emerging exploitation platforms you learn that the genius in cyber threat intell lies in conducting your research without contributing to the cybercrime ecosystem by purchasing any of the releases - which is exactly how this analysis was conducted.

The Chimera botnet is courtesy of a Russian vendor developing web applications and backend systems for botnets, with a particular emphasis on coding malware for hire. Some of their most notable (public) releases include [performance-boosting modifications](#) within the Zeus crimeware kit, the introduction of a [carding-theme within the kit](#) (now an inseparable part of all the new versions), and integrating a [MP3-player/online radio feature](#) within the crimeware kit. The managed service offers two versions in a typical modular-malware fashion in this case for spamming and launching DDoS attacks, with the backend's interface exclusively based on the ExtJS AJAX framework, with the malware itself compatible with Windows

SP sp1/2/3, and Windows Vista with the authors claiming it will run as an authorized application.

Go through related Cybercrime-as-a-Service posts: [The Neosploit cybercrime group abandons its web malware exploitation kit](#) ; [Cybercriminals release Christmas themed web malware exploitation kit](#) ; [Crimeware tracking service hit by a DDoS attack](#)

How much did the BBC pay for access to the managed botnet, and what are the chances that the sellers are involved in a countless number of hardcore cybercriminal activities? Interestingly, the (now down) vendor's site isn't exclusively offering the 20k infected hosts that the BBC purchases, thereby leaving the possibility for what may look like [an overpriced deal](#) . However, a price of \$400 for a particular managed malware binary is cited, with the size of botnet changing proportionally with the vendor's malware campaigns circulating in the wild.

The whole "botnet fiasco" puts the spotlight on a dynamic cybercrime ecosystem with well-known vendors clearly working with one another. In this particular case, the vendor of the Chimera botnet is part of an affiliate network offering "[localization on demand](#) " services, namely, capable of empowering a Chinese cybercriminal with the ability to translate all of his spam/malware/phishing campaigns to a language of his choice, breaking the language barrier which often indicates the real origin of the campaign.

The [disturbing part](#) with such "[malware for hire](#) " and "botnets for rent" services is their emphasis on standardization which results in efficiencies and efficiencies themselves in cost-effective scalability. For instance, asked by a customer whether or not their backend can handle more than 50k of infected hosts before requesting a customer-tailored interface, the vendor responds that the last big botnet that they ported costing of 1.2 million hosts was working "just fine".

The Chimera botnet's vendor is currently in a cover-up mode, monitoring of their releases would continue.

Inside an affiliate spam program for pharmaceuticals | ZDNet

Bargaining with your health doesn't just mean you're heading for a shorter life expectancy, but also, increases the chances that you will either get scammed in the process, or have to pay more in the long-term while dealing with the health issues arising from using expired pharmaceutical with unverifiable origins, you bargained for at the first place.

Just like vendors of rogue security software and system utilities software contributing to the increase of cybercrime activities due to the high payout rates enticing the affiliate network's participants to spam, engage in blackhat SEO and SQL inject sites to redirect the visitors to the scam domains, pharmaceutical affiliate programs do exactly the same by allowing spamming, blackhat SEO, botnet traffic through redirects, and due to high amounts of money they make - directly advertise the scam sites on the major search engines.

Out of the close to a hundred (100) unique pharmaceutical spam affiliate programs currently operating, let's find out what is driving the increasing levels of pharmaceutical spam by taking an inside peek at such a program operating since 2003, whose advertisements speak for themselves in terms of revenues - *"Around 50 Americans (85% of their sales) purchase pharmaceuticals from their affiliates on an hourly basis"*.

The underground ecosystem for pharmaceutical spam is analogical to that of legitimate online shops, since it's successfully scaling just like they do - through affiliate based programs where the scammers share revenues with the participants who will undertake a great deal of illegal activities while earning high commissions in the process.

It's also worth pointing out that despite the program's claims that it doesn't endorse spam and traffic coming from botnets on its web page, some of the program's managers have exactly the opposite

attitude across multiple forums - they don't mind. Here's how the process works :

1. Affiliates will receive an assigned code upon signing up for the affiliate program. That code is used to track all sales to adequately compensate affiliates. The code must be used as provided. Any altering of the code may result in inaccurate tracking and in some cases may constitute fraud. Affiliates are only allowed to use approved advertising banners and materials. Any affiliate wishing to create their own advertising materials must get explicit permission to do so in advance of using any such materials. Not gaining permission to do so may be grounds for termination from the program and forfeiture of any monies due

2. Payouts will be made weekly on Tuesday for the week before previous. I.e., all earnings from monday to sunday of 1st week would be paid on the Tuesday of the 3rd week. The minimum payout is \$100. If the minimum is not reached during the pay period, the amount will be rolled over until minimum is made. We pay out by bank wire transfers, WebMoney, and Fethard. The wire cost is \$15. Wire is free for payments above \$1000

3. Affiliates may not make any unfounded claims about our product, company, website, affiliate program or transactions. Affiliates also may not make any false claims regarding prices

4. Any means of attempting to cheat our program or our customers in any way will result in immediate termination with forfeiture of all monies due. Anyone terminated from our program for non-compliance of our terms will also be unable to participate in any other promotion or affiliate program we own and or operate

So once you've been approved as an affiliate and receive your unique tracking code, you're free to choose the pharmaceutical products, pick up the creative and choose of the many templates for online pharmacy shops, then start driving traffic to them. Some affiliate programs add value to the registration process by introducing ratio calculators in order to make it easier for new participants to calculate their earnings based on the selling price that they choose for the item. Pretty simple, and that's the problem, since

anything required for the participant [to drive traffic and monetize it](#) , can be, and is [easily outsourced](#) .

What about the big picture? [MarkMonitor's Summer 2008 Brandjacking Index](#) , covers in-depth [the proliferation of pharmaceutical scam sites](#) , and points out that despite the fact that the total number of unique online pharmacies is decreasing, the traffic to the remaining ones triples due to the combination of traffic acquisition tactics applied by the participants of the affiliate programs. Here are some of the key summary points regarding their analysis of the current situation :

Of the 2,986 online pharmacies studied, only two are Verified Internet Pharmacy Practice Sites (VIPPS), the industry credential that assures consumers of legitimate online pharmacy operations. More than one-third of the online pharmacies in the study generate enough traffic to merit an Alexa ranking. Each of these sites sees an average of 99,000 visitors daily, more than triple the daily visitors noted in 2007. Using industry statistics for traffic conversion and average order sizes, MarkMonitor estimates that this traffic converts to \$12 billion in annual sales for the six drug brands studied, an increase from the 2007 estimate of \$4 billion.

Marketers for these pharmacies and sites are becoming increasingly aggressive. MarkMonitor estimates brandjackers spend \$26 million annually for search advertising using only those six keywords.

Representative sampling of pricing for one popular drug brand shows an 85% average price discount at illicit pharmacies when compared to certified pharmacies.

64 percent of these 2,986 pharmacies do not secure customer data, putting consumers' identity information at risk. This number has grown compared to 50 percent last year.

49 percent of the 2,986 pharmacies were hosted in the U.S., followed by the U.K., which hosted 12 percent, and Germany, which hosted 9 percent.

Exchange sites that sell pharmaceuticals in bulk quantities by the pill as well as sell active pharmaceutical ingredients (APIs) risk corrupting the overall drug supply chain. Analysis of just 40 listings on exchange and trade sites shows a \$30 million wholesale market for the six brands studied.

60 percent of pharmacies identified in 2007 are still operating, and 59 percent of online exchange listings identified in 2007 remain active

With [more surveys indicating](#) that users are [buying from spammers](#) , just ask yourself the following before purchasing pharmaceuticals in this particular case - how is it possible that the vendor is offering 45% payout rate and up to 85% average price discount compared to legitimate pharmacies? Pretty simple, [since you're never going to receive anything](#) else from them, but a a billing entry on your bank statement :

"Here is an example of one online pharmacy that is labeled as Canadian but hosted in the Russian Federation, according to its IP address. Last year, it listed a Los Angeles area code, but this year the company shows a Texas phone number. We made a purchase from this website and our credit card statement reflects an Israeli merchant account; as of our publication date, the drugs have not been delivered. No matter where its real location is, it continues to display faked credentials, and when you telephone them, a heavily-accented Russian voice invites you to leave a message."

And even [if you're lucky enough to receive something](#) , using the prescription drugs obtained without a prescription when shipped from India, might not be such a good idea.

With the ever-decreasing costs of spamming due to the efficiencies achieved by the [managed spamming providers](#) , the very few purchases out of the hundreds of thousands of spammed potential customers will remain sufficient revenue in order for spammers to break-even, and profit out of these very few people.

Images (excluding the affiliate program screenshots) courtesy of [MarkMonitor](#) , [Spamdontbuyit.org](#) and [Modern Life](#) .

India's government: At last, we've cracked Blackberry's encryption | ZDNet

Following India's [threat to shut down the Blackberry network in the country](#) unless Research in Motion allows the government to snoop on Blackberry users made earlier this year, the country seems to have found a more pragmatic solution, and in a surprising move has publicly announced that they have [finally managed to crack Blackberry's encryption](#) :

"The government has decrypted the data on Research In Motion's (RIM) BlackBerry networks. The department of telecommunication (DoT), Intelligence Bureau and security agency National Technical Research Organisation (NTRO) have done tests on service providers such as Bharti Airtel, BPL Mobile, Reliance Communications and Vodafone-Essar networks for interception of Internet messages from BlackBerry to non-BlackBerry devices.

Initially, there were difficulties in cracking the same on Vodafone-Essar network but that has also been solved. This means that the e-mail messages sent on Internet through your BlackBerry sets would no longer be exclusive and government would be able to track them."

They either need to decompress, or emphasize on the fact that their efforts cannot affect BlackBerry Enterprise Service users.

The government's "decompression tests" seems not to be affecting enterprise Blackberry solutions, but now that it's becoming clear that they're requiring all local telecoms to "make technical changes in their services to make them compatible for decompression", the tests indicate that the government is on purposely weakening the security of transmitted data across the country.

Taking into consideration the multi-layered end-to-end encryption that a Blackberry user can archive, India's claims to be able to eavesdrop Internet traffic of BlackBerry Internet Service, but naturally still unable to crack BlackBerry Enterprise Service's end-to-

end AES or Triple DES, doesn't really count as cracking Blackberry's encryption.

ImageShack hacked by anti-full disclosure movement | ZDNet

During the weekend, ImageShack, among the Web's top ten most popular free image hosting services got compromised, with the millions of images hosted on it redirected to a single one explaining why it was hacked.

The anti-sec group responsible for the compromise describes itself as a "*movement dedicated to the eradication of full-disclosure* ", has also threatened web sites and communities publishing exploits in a full-disclosure fashion.

The message left in the form of an image reads:

"Full-disclosure is the disclosure of exploits publicly - anywhere. The security industry uses full-disclosure to profit and develop scare-tactics to convince people into buying their firewalls, anti-virus software, and auditing services.

Meanwhile, script kiddies copy and paste these exploits and compile them, ready to strike any and all vulnerable servers they can get a hold of. If whitehats were truly about security this stuff would not be published, not even exploits with silly edits to make them slightly unusable."

Whereas this radical -- and illegal -- approach of spreading a philosophy aims to put the spotlight on the full disclosure debate for yet another time, things have greatly changed during the past couple of years, potentially rendering their efforts pointless, at least from the perspective of using zero day exploits for committing cybercrime. The very notion that the well known exploits-repository web sites are the original point of publication for a particular exploit is naive. Case in point - the recent thought to be "zero day" Video ActiveX Control flaw, has been [reported to Microsoft over an year ago](#) , but it became an inseparable part of a Chinese-based malware campaign earlier this month.

Moreover, not only did [vulnerability markets](#) and market approaches to [software vulnerability disclosure](#) greatly [improved](#) ,

but also, the active [OTC \(over-the-counter\) market for vulnerabilities](#) has once again proved that what's a zero day flaw for some, is last month's zero day used by a particular cybercriminal in targeted malware attacks.

The anti-sec group also makes a statement in respect to the *"script kiddies who copy and paste these exploits and compile them, ready to strike any and all vulnerable servers they can get a hold of."* Shouldn't this also be the practice of the people responsible for the security of a particular web property as well, and if exploitation is possible, a patch or alternative mitigation strategy applied as soon as possible? Who's to blame in this case, the lack of self-awareness on behalf of the affected sites ending up as the "low hanging fruit", or the site providing the service that inevitably improves the effectiveness of ethical penetration testing tools if used at the first place?

Ironically, cybecriminals do not need zero day exploits in order to continue efficiently infecting users of compromised web sites due to a simple fact - the end user's host is already using a multitude of [outdated and easily exploitable applications](#), patches for which are available, but haven't been applied. Take [Conficker for instance](#), even through an out-of-band patch was released, a [huge percentage of hosts remained unpatched](#) for months to come. The web malware exploitation kits currently in circulating, rely on anything else but zero days in order to successfully infect end users, since their authors embraced a simple fact - that diversification of the exploits set in popular applications increases the probability of infection.

What do you think? Is this one of those black and white situations where full-disclosure should be replaced with responsible disclosure, or is full-disclosure in fact serving the community, especially considering the fact that cybercriminals are efficiently infecting hosts by exploiting already patched and outdated flaws and do not necessarily need a zero day to do so?

Talkback.

iHacked: jailbroken iPhones compromised, \$5 ransom demanded | ZDNet

Yesterday, a "Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your phone right now!" [message popped up](#) on the screens of a large number of [automatically exploited Dutch iPhone users](#), demanding \$4.95 for instructions on how to secure their iPhones and remove the message from appearing at startup.

Through a combination of port scanning and OS fingerprinting of T-Mobile's 3G IP range, a Dutch teenager has for the first time [automatically exploited a known security vulnerability introduced on jailbroken iPhones](#) - the SSH daemon which unless modified remains running with default users root and mobile, using the same password on each and every device.

Here's what he demanded, and how he changed his attitude following the suspension of his PayPal and the spamvertised URL:

The now taken offline site was featuring [the following message](#) :

"Dear iPhone user,

Your iPhone is not secure. That's the reason your visiting this page, isn't it? Well you can pay me \$4,95 at my paypal account PureInfinity92@mailinator.com, and I'll mail you very easy instructions on how to secure your iPhone. You can also contact me at PureInfinity92@gmail.com

If you don't pay, it's fine by me. But remember, the way I got access to your iPhone can be used by thousands of others. And they can send text messages from your number (like I did..), use it to call (or record your calls), and actually whatever they want, even use it for their hacking activities! I can assure you, I have no intention of harming you or whatever, but, some hackers do! It's just my advise to secure your phone (: Have a nice day!"

Following the media coverage, active discussions across popular Dutch IT forums, and the timely shut down of his PayPal account,

the opportunistic and unethical pen-tester quickly [changed his attitude and posted an apology](#) followed by [step-by-step guide on changing the default SSH password](#) , which he was originally offering for a fee.

Why is this automatic exploitation not a surprise?

Go through related posts: [iBotnet: Researchers find signs of zombie Macs](#) ; [iPhone's anti-phishing protection offers inconsistent results](#) ; [Snow Leopard's malware protection only scans for two Trojans](#) ; [New Mac OS X DNS changer spreads through social engineering](#)

The exploitability of the default SSH root login combined with the [ease of OS fingerprinting an iPhone's](#) , and the descriptive and well known 3G IP ranges for certain service providers, has already been discussed as an opportunity for [automatically exploiting jailbroken iPhones running the SSH daemon with default passwords](#) .

IE8 outperforms competing browsers in malware protection -- again | ZDNet

A recently released [study by NSS Labs](#) is once again claiming that based on their internal tests, Microsoft's Internet Explorer 8 outperforms competing browsers like Google's Chrome, Mozilla's Firefox, Opera and Apple's Safari in terms of protecting their users against "[socially engineered malware](#)" and [phishing attacks](#).

Not only did IE8 top the chart, but also, the rest of the browsers have in fact degraded their "socially engineered malware" and phishing block rate in comparison to the results released by the company in the [March's edition of the study](#).

How objective is the study? For starters, it's Microsoft-sponsored one. Here's how it ranks the browsers:

Socially engineered malware block rate:

Microsoft Internet Explorer v8 - 81% block rate
Mozilla Firefox v3 - 27% block rate
Apple Safari v4 - 21% block rate
Google Chrome 2 - 7% block rate
Google Chrome 2 - 7% block rate

Phishing attacks block rate:

Microsoft Internet Explorer v8 - 83% block rate
Mozilla Firefox v3 - 80% block rate
Opera 10 Beta - 54% block rate
Google Chrome 2 - 26% block rate
Apple Safari v4 - 2% block rate

What is "socially engineered malware" anyway? Basically, it's the direct download dialog box that appears on a, for instance, scareware or [Koobface video page](#) spoofing Facebook's layout, like the one attached. using "socially engineered malware" as a benchmark for malware block rate isn't exactly the most realistic choice in today's threatscape.

And even if it is, some pretty realistic conclusions can be drawn by using some internal traffic statistics from [Koobface worm's](#) ongoing malware campaigns. The [Koobface worm](#) , one of the most efficient social engineering driven malware, is a perfect example of how security measures become obsolete when they're not implemented on a large scale. The stats themselves:

- MSIE 7 - 255,891 visitors - 43.33% - MSIE 8 - 189,380 visitors - 32.07% - MSIE 6 - 76,797 visitors - 13.01% - Javascript Enabled - 585,374 visitors - 99.13% - Java Enabled - 576,782 visitors - 97.68%

What does this mean? It means that with or without the supposedly working "socially engineered malware" block filter using a modest sample of several hundred URLs, the Koobface botnet is largely driven by MSIE 7 users. The irony is that [the previous edition of the study](#) dubbed IE7 a browser which "practically offers no protection against malware" with the lowest block rate achieved back then - 4%.

Just like the previous edition of the study, this one also excludes the notion that client-side vulnerabilities ([Secunia: Average insecure program per PC rate remains high](#) ; [Secunia: popular security suites failing to block exploits](#)) continue contributing to the "rise and rise" of [web malware exploitation kits](#) . By excluding client-side vulnerabilities, the study isn't assessing IE8's [DEP/NX memory protection](#) , as well as omitting [ClickJacking](#) defenses and [IE8's XSS filter](#) , once pointed out as a [less sophisticated alternative](#) to the Firefox-friendly NoScript.

Socially engineered malware is not the benchmark for a comprehensive assessment of a browser's malware block rate. It's a realistic assessment of the current and emerging threatscape combined with comprehensive testing of all of the browser's currently available security mechanisms, a testing methodology which I think is not present in [the study](#) .

IE7 XML parsing zero day exploited in the wild | ZDNet

A couple of hours ago, two [working proof of concept exploits](#) for MS Internet Explorer XML Parsing Remote Buffer Overflow were posted at Milw0rm, with international hacking communities quickly catching up and starting to use it. [The second PoC also works on Vista](#), in particular both exploits were tested on Vista SP1, Explorer 7.0.6001.18000, Vista SP0 Explorer 7.0.6000.16386, and also on WinXP SP3, Explorer 7.0.5730.13.

And if that's not enough, Microsoft is also investigating a second [zero day affecting the WordPad text converter](#) according to an advisory issued yesterday.

Not surprisingly, the IE7 exploit is already in circulation, with [the Shadowserver Foundation](#) keeping track of malicious domains using it, the majority of which still remain active. Despite the fact the in its current form [the exploit code](#) is easy to spot through [generic detection](#) for potentially malicious shellcode, sampling several of the domains using it reveals that the Chinese hackers using it are also taking advantage of several different client-side vulnerabilities in order to increase the chances of successful infection. Typical exploits structure looks like the following :

baidu .bbtu01. cn/c0x.htm baidu. bbtu01. cn/ie07.htm baidu. bbtu01. cn/104.htm baidu. bbtu01. cn/a0s.htm baidu. bbtu01. cn/c0e.htm baidu. bbtu01. cn/lzz.htm baidu. bbt u01 . cn/Bf0yy.htm baidu. bbtu01. cn/rea0l10.htm baidu. b btu01. cn/real11.htm

Despite that the malicious domains remain injected at legitimate Chinese sites and forums as iFrames only, this could easily change so that more legitimate international sites start getting targeted. What are they after this time? [Passwords for popular online games in China](#) .

ICANN warning against registrar impersonation phishing attacks | ZDNet

How realistic is an attack that successfully hijacks a domain by social engineering the domain's registrar? Pretty realistic according to ICANN's recently released advisory on [preventing Registrar Impersonation Phishing Attacks](#) :

In this Advisory, SSAC describes generic forms of this type of attack. We

consider types and formats of information included in legitimate email messages that various registrars use when corresponding with customers. We discuss how phishers manipulate these information types and formats to create a bogus correspondence that is designed to socially engineer¹ the registrar's customer into visiting an impersonated registrar web site. The attacker designs the impersonated web site to dupe the customer into disclosing domain management account names and credentials. We discuss some of the current recommended practices to minimize or prevent phishing attacks employed by common phishing targets such as financial institutions and large corporations. We recommend measures that registrars can take to make their correspondences with registrants less "phishable" and identify ways for registrants to detect and avoid falling victim to this form of phishing.

Some of the most notable cases of domain hijacking through impersonation of the real owner in order to socially engineer the registrar to give up to domain, are the [Panix.com incident](#) (2005), [Hushmail.com incident](#) (2005), as well as, Sex.com, Nike.com and Ebay.de all have been victims of domain hijacking, the details of which you can find in a detailed retrospective of [Domain Hijacking](#) .

The attacks rely on basic social engineering tactics such as visual spoofing of the registrar's login page, personalization in the phishing email send to the registrant using the data obtained from the public WHOIS record for the domain owner. What follows is a targeted

mailing of the phishing email including a the typical phishing URL in the following format :

myaccount.session-83040251 .godaddy.com.
nextid.li/AccountConfirmation/account.aspx myaccount.session-
8787227 .godaddy.com. filxcii.tv/AccountConfirmation/account.aspx
myaccount.session-10677 .godaddy.com.
userport.li/AccountConfirmation/account.aspx myaccount.session-
6104002 .godaddy.com. iriikfrt.ch/AccountConfirmation/account.aspx
myaccount.session-83040251 .godaddy.com.
nextid.li/AccountConfirmation/account.aspx

The advisory contains some practical tips for both, registrars and registrants on protecting against such social engineering attempts, so [consider going through it](#) .

ICANN terminates EstDomains, Directi takes over 280k domains | ZDNet

Following ICANN's notice of termination sent to [cybercrime-friendly domain registrar EstDomains](#) in October, on the 24th of November the termination became a reality and [EstDomains is no more](#) . Despite the public concerns of who will take the 280,000 domains, and that includes the cybercrime facilitating ones, [Directi's ResellerClub](#) is new home for [EstDomains customers](#) .

ICANN's **Stacy Burnette** , Director of Contractual Compliance, was kind enough to elaborate a little bit more on ICANN's decision to terminate EstDomains, and how is the bulk transfer of their domains portfolio going to benefit the community.

Go through the Q&A.

Q: Terminating EstDomains accreditation is indeed a step in the right direction, but isn't it a bit disturbing that what prompted the ICANN to do it wasn't the fact that the registrar was facilitating the registration of hundreds of thousands of cybercrime driving domains, but their CEO's earlier conviction? Would EstDomains be still in operation if the ICANN wasn't aware of the conviction?

A: ICANN is not a law enforcement authority and an allegation that a registrar is "facilitating the registration of hundreds of thousands of cybercrime driving domains" is not grounds for termination under the [Registrar Accreditation Agreement \(RAA\)](#) .

Most RAA violations require ICANN to send the registrar notice of breach and provide the registrar an opportunity to cure the breach. If the registrar cures the breach within the time period provided in the RAA, the matter is closed. There are very few RAA violations that are terminable and do not allow the registrar to cure. Pursuant to Section 5.3 of the RAA, the conviction of a registrar officer is one of the few contract violations that allows ICANN to terminate without an opportunity for the registrar to cure. Although RAA amendments intended to provide [additional enforcement tools are currently under](#)

[consideration](#) , ICANN will continue to use the enforcement tools available in the RAA.

Q: A large percentage of EstDomains' portfolio is still comprised of the cybercrime facilitating domains, which is natural despite the fact that they will no longer be allowed to slow down the shut down process. Do you believe that the bulk transfer of their legitimate and fraudulent domains to a more cooperative domain registrar in the face of Directi, would make the impact the security community and the average Internet user wants to see in general?

A: Directi representatives have expressed an openness to work collaboratively with the security community to analyze the domain name registrations formerly managed by EstDomains and take action where there is proof that the domain name registrations are being used for unlawful purposes. The security community and the global Internet community benefit from such cooperation. ICANN commends Directi for its willingness to work with the security community and encourages other registrars to do the same.

Q: Having monitored a dozen of anti-abuse hosting providers throughout 2008, and continuing to do so, while their hosting services allow malware, logs of stolen e-banking details, and malicious redirection scripts only for "starters" they exclusively forbid other cybercriminals from hosting child pornography, pirated software and in fact entice them to enter "correct" Whois information so that they can ensure the domains remain online longer.

From a legal perspective, does the ICANN have any authority over cybercrime domains hosting underground data over which ICANN's rules perhaps doesn't apply? Moreover, does ICANN's long-term vision have to do with more policing or better cooperating with the security community as an early warning system?

A: You asked if ICANN has "any authority over cybercrime domains hosting underground data over which ICANN's rules perhaps doesn't apply." ICANN is a technical coordination body with responsibility for, among other things, overseeing the domain name registration system and ensuring that all ICANN-accredited registrars comply with the provisions of the RAA.

ICANN has consistently worked cooperatively with the security community to address a variety of security issues. In the past, ICANN has received information from the security community and ICANN has used that information constructively to address issues that fall within its mission and authority. ICANN will continue to work collaboratively with the security community to effectively address security related issues.

Q: Bulk domain registrations are systematically abused for cybercriminals on a daily basis. In fact, I can easily argue that the average time it takes to track, report and shutdown such a domain portfolio is enough for them to break even and scam several thousand people on average depending on the volume and scale of their attack tactics. With cybercriminals systematically exploiting domain registrars with weak anti-abuse practices, isn't it time for a major clean-up operation of such registrars?

A: Note your opening discusses registrations but your question deals with registrars. ICANN encourages registrars to implement anti-abuse policies that result in the swift cancellation of domain names used for unlawful purposes. This is an area where greater collaboration between ICANN and the registrar community is needed to develop better registrar practices.

The bottom line is that when a trusted and actively cooperating with cybercrime fighters and security researchers domain registrar starts managing EstDomains portfolio, there's a higher chance for faster takedowns of malicious domains. In Directi's case, [their cooperation with the community](#) has been pretty evident. For instance, in October alone [they've suspended over 175,000 domains](#) due to fake whois entries, spam, phishing and pharmaceutical hosting involvement, and I'm sure the numbers are only going to get better.

ICANN and IANA's domains hijacked by Turkish hacking group | ZDNet

What happens when the official domain names of the organizations that issue the domain names in general, and provide all

the practical guidance on how to prevent DNS hijacking, end up having their own domain names hijacked? A wake up call for the Internet community.

The official domains of [ICANN](#) , the Internet Corporation for Assigned Names and Numbers, and [IANA](#) , the Internet Assigned Numbers Authority were hijacked earlier today, by the NetDevilz Turkish hacking group which also [hijacked Photobucket's domain](#) on the 18th of June. [Zone-H mirrored the defacements](#) , some of which still remain active for the time being :

The ICANN and IANA websites were defaced earlier today by a Turkish group called "NetDevilz". ICANN is responsible for the global coordination of the Internet's system of unique identifiers. These include domain names, as well as the addresses used in a variety of Internet protocols. The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources.

NetDevilz left the following message on all of the domains :

"You think that you control the domains but you don't! Everybody knows wrong. We control the domains including ICANN! Don't you believe us? haha :) (Lovable Turkish hackers group)"

The following domains were hijacked, and some of them still return the defaced page - [icann.net](#) ; [icann.com](#) ; [iana-servers.com](#) ; [internetassignednumbersauthority.com](#) ; [iana.com](#) .

The hackers are once again redirecting the visitors to **Atspace.com** , **82.197.131.106** in particular, the ISP that they

used in the Photobucket's DNS hijacking. And while Photobucket hasn't issued an official statement on the DNS hijack, **Atspace.com**

did so last week, [a copy of which you can find here](#) .

The NetDevilz hacking group seems to be taking advantage of a very effective approach when hijacking domain names, and while they declined to respond to an email sent by Zone-H on how they did it, cross-site scripting or cross-site request forgery vulnerability speculations are already starting to take place.

One thing's for sure though, if the ICANN and IANA can lose control of their domains, anyone can.

Hundreds of high profile sites unprotected from domain hijacking | ZDNet

A [MarkMonitor review of](#) the adoption of [VeriSign's Registry Lock Service](#) launched at the beginning of the year, shows that less than 10% of the top 300 most highly trafficked sites were protected using it.

Should a company entrust the integrity of its high value Web property to a domain registrar, or a DNS service provider in the wake of the most recent [Twitter](#) and [Baidu](#) domain hijackings? How much damage can be done to brand's reputation in an event of domain hijacking? Where's the weakest link?

Go through the Q&A with Elisa Cooper, Director, Product Marketing, at MarkMonitor.

Were you surprised to find out that less than 10% of the 300 top high trafficked web sites were using the newly introduced "Registry Lock Service"?

Elisa: I was disappointed to see that the adoption of this service was so low, but not entirely surprised because most registrars are not actively promoting or even offering it, in many cases.

What exactly is the VeriSign's Registry Lock Service, and how does it differentiate itself from the already established services offered by a domain registrar?

Elisa: Unlike security options offered by registrars, VeriSign's Registry Lock Service secures domains at the registry-level. The only way domains with this setting can be updated is if the registrar contacts VeriSign and completes a specific set of security protocols.

So even if a registrant's credentials are compromised, or hackers infiltrate a registrar's back-end system, domains with this security setting can not be updated in any way. At MarkMonitor, only a limited number of individuals know how to complete this set of security protocols to add a further check-and-balance to the process.

Why do you think the companies remain reluctant to implement the service? Lack of awareness building on its existence, or a false feeling of security offered by the protection currently in place on their domain registrars?

Elisa: I think that a number of factors are in play. While this service is not actively promoted or offered, even by corporate-only registrars, due to the added responsibility of working directly with the registry to complete legitimate updates, the bigger issue is that many high-profile domains are still registered with retail registrars.

The business models of retail registrars are focused on providing high-volume, highly-automated registration services and this type of security solution falls outside that model. Retail registrars would find it extremely difficult, if not impossible, to offer such a service.

How much damage do you think can be caused to a brand's reputation in case of a DNS hijacking incident? Is the negative publicity a short-lived PR disaster, or do you think there are other long-term negative issues that the company is facing?

Elisa: If a website is only providing information, and is not collecting credential information, I think that the harm caused is likely to be short-lived. However, for sites collecting credential information - even basic information like a username/password combination - or conducting transactions, I think that effects could be longer lasting as visitors of the affected site may be reluctant to provide sensitive information fearing that they may have fallen prey to a phishing scam.

Despite the fact that so far, we haven't seen embedded malware attacks in any of the high profile DNS hijacking incidents, how realistic do you think is a scenario where the attackers move beyond their hacktivist ambitions, and go truly malicious? Would such an event drive growth in the adoption of Registry Lock Services?

Elisa: I definitely think that is possible, and I am frankly surprised that we haven't seen these types of attacks yet. I would hate to have to come to the point where this type of event is the driving factor for the adoption of this service.

Where's the weakest link? The domain registrar, the domain registrant, or both are equally susceptible to the social engineering attacks most commonly used in the successful DNS hijacking incidents?

We've seen instances of attacks targeted at both the registrant and the registrar. Although the registrants of highly-trafficked domains are sophisticated and would not likely fall prey to simple phishing scams, I am concerned about the possible use of keyword loggers to collect credential information to access domain management portals.

I think also that domains that are registered by large retail registrars are also highly vulnerable to social engineering attacks. At this point, I'd say that both are equally vulnerable but that there are a number of security measures that can be implemented including Two-Factor authentication of users, restrictions to online management tools by IP Address, and of course, VeriSign's Registry Lock Service.

Consider going through related posts on high profile DNS/Domain hijackings from the past two years, including details on how the incidents took place:

[ICANN and IANA's domains hijacked by Turkish hacking_group \(June, 2008\)](#) [Photobucket's DNS records hijacked by Turkish hacking_group \(June 2008\)](#) [Comcast's DNS records hijacked, redirect to hacked page \(May, 2008\)](#) [Hackers hijack DNS records of high_profile New Zealand sites \(April, 2009\)](#) [Twitter's DNS records hijacked \(December, 2009\)](#) [Baidu DNS records hijacked by Iranian Cyber Army \(January, 2010\)](#)

The message from [MarkMonitor's findings](#) is clear - leaving [the faith of your Web property into the hands of a domain registrar or a DNS service provider](#), is the worst thing you could do given the availability of additional layers of security.

Hundreds of Dutch web sites hacked by Islamic hackers | ZDNet

In what appears to be a mass defacement, where several hundred domains take advantage of a shared hosting provider,

starting as of this Friday, an [Islamic hacker known as nEt^DeViL](#) -- this is not the NetDevilz team that [hijacked the DNS records](#) of the ICANN and [Photobucket](#) in June -- managed to successfully hack a couple of hundred Dutch web sites as a [hacktivist](#) response to the release of the [Fitna film](#), a controversial film released by Geert Wilders, a member of the Dutch parliament in March, 2008.

How did they do it? Since all of the sites are parked on a single IP (**81.4.97.190**) owned by the **Geenpunt.nl** hosting company, compromising it means having the ability to compromise the content on all the domains hosted there, which is exactly what happened in this case.

The message they left is still active at most of the sites :

"Anti-Fitna (Response to the Fitna Movie by 'Geert Wilders' Cow !) This hax0ring is to defend ISLAM - The Religion of [Abraham, Moses, Jesus & Muhammad (Peace Be Upon Them All)] that Insulted by a Cow ! from Netherlands ! Show Some Respect ! so , I can Leave you in Peace ! [You've Started it !] , I don't have problems with your site but, that what Geert Wilders Cow! chose for you ;) If you think that " Insulting GOD Religion is a Freedom of Speech as your country did , then allow me to show you my Freedom knowledge of Hacking ;) "

[by the way, nothing was deleted relax ^_^ only your index renamed][NO

WAR] ... [NO HATING] ... [NO Lammers !] ... [NO Subdirs ;)] Can Break Your Lame Security ! [Love Coding than Hacking ;) ' Perl , Python , PHP, JavaScript , HTML, VB , Borland Delphi, a Little of C/C++ & Assembly ']

aB0 m0h4mMed .. for the Old Times Greetings & Peace to my Brothers. Abu_Zahra[My Best friend] ? Saudia_Hacker ? Abu Lafy ? DeadLine , DosMan & b0hAjEr [Q8Crackers Crew] ? Yanis ? Broken-Proxy ? Eddy_BAck0o ? Mianwalian & ZeRo from [#WHACKERZ] ? SaveChanges[PHA] ? FBH Crew ? Apocalypse ? PaKBrain ? DaVenjah! ? BrEakerS ? Red Devils Crew[Saudi|x] ? by_emR3 , Kerem125 , Gsy & Alemin Krali [Gr347 7urk15h |3ro7h3r5] ? sys-worm(turkish) ? F10 ? ZombiE_KsA ? xOOmxOOm net_devil@hackermail.com"

Naturally, this isn't the first time Islamic hacking groups attacked web sites belonging to a particular country that somehow offended their beliefs. For instance, in 2006, the same [mass defacements took place on over 600 Danish web sites](#) in response to the [Mohammed's cartoons](#) released in local newspapers. This hacktivist approach of spreading propaganda isn't necessarily a full-scale cyber war, it's an example of information warfare aiming to reach as many Dutch Internet users as possible due to the apparently insecure web hosting provider that they are all using.

Pure hacktivism isn't dead, as compared to previous [web site defacement analysis](#) where the people behind them were

multitasking by also [hosting malware, phishing and blackhat SEO junk pages on the compromised servers](#) , in this case they only defaced the main pages. However, what pure hacktivism turned into today, consciously or subconsciously, is the propaganda division of an information warfare unit, where given the hundreds of thousands of easily detectable insecure sites within a particular country's Web, this political propaganda can easily turn into a large scale malware attack.

As in real life through, the real cyber conflicts usually start due to such provocations where a single group or a script kiddie's actions can cause a lot of damage if that's what they want to achieve at the first place.

Related posts:

[Pro-Serbian hacktivists attacking Albanian web sites](#) [300 Lithuanian sites hacked by Russian hackers](#) [Georgia President's](#)

[web site under DDoS attack from Russian hackers](#) [Coordinated Russia vs Georgia cyber attack in progress](#)

HSBC sites vulnerable to XSS flaws, could aid phishing attacks | ZDNet

What would the perfect phishing attack from a social engineering perspective? The one that compared to using typosquatted domains impersonating the bank's web application directory structure is in fact using the bank's legitimate domain names as redirectors due to XSS flaws within. It's even more interesting to measure the average time it takes for a bank to fix the XSS flaws within its sites upon getting notified of them, which in some cases is longer than the average time it takes to shut down a phishing site.

In [yet another compilation of XSS vulnerable sites](#) courtesy of Dimitris Pagkalos at [XSSed.com](#), the largest online archive of XSS vulnerable websites, HSBC Holdings plc owned domains are vulnerable to XSS flaws which could easily aid in a phishing attack :

"Evidently, major unwanted consequences could be a result of multiple cross-site scripting vulnerabilities affecting bank web sites. XSS must be considered as the phishers' future weapon by all people working in the security industry. Scammers can register domains and set up fake bank web sites in a few minutes. With the help of bulk e-mailers they can phish personal sensitive data from thousands of unsuspecting web users.

If they want to own HSBC's e-banking customers, all they have to do is to register a "suspicious" looking domain like hscsbc.com which is currently available and then serve a phishing page. Even better, they can exploit a cross-site scripting vuln on hsbc.com, obfuscate the attack vector and significantly increase their phishing success rate!"

With the Ebanking industry slowly embracing the "[No Security Software, no Ebanking Fraud Claims for You](#) " mentality in order to forward the risk of potential fraud claims to the customer, would a customer still be able to file fraud claims given that the phishing attack occurred due to a vulnerability in the bank's site? They'll

definitely ask for the security software in place before that, indicating their degree of NOT understanding the threats to their customers.

A brief excerpt from the previous post on the irrelevance of having security software in place when the bank's sites are vulnerable, and why the emphasis on the security software speaks for the simplistic understanding of the threats their customers face on a daily basis :

"Cross-site scripting [vulnerabilities within banking sites](#) are nothing new, in fact, in the past there were initiatives tracking down such vulnerabilities and how long it took for the bank to fix them. [Barclays is an example with XSS vulnerabilities](#) unfixed for over a year despite notification. Why aren't they taking XSS seriously at the first place? Because the people responsible for their anti-fraud activities aren't aware of the potential to abuse the vulnerabilities and use the bank site as a redirector to malicious software, or a phishing page with a decent SSL certificate in place. [Phishers are indeed using XSS vulnerabilities](#) to scam a bank's customers, thanks to the bank's vulnerable web applications, here's [the most recent incident](#) "

It always starts with the basics. A customer should demand some accountability from the banks he's using on what are they doing to make his transactions more secure, and [what have they done for the past couple of years](#) in this direction. The reality is that the banks themselves don't make a difference between a Trojan horse and a banking malware, it's all viruses to them, and this underestimation of the current threatscape directly reflects their inability to protect their customers. Here are some examples in regard to HSBC for instance :

- The [importance of patching is limited to visiting the Windows Update site](#) , which leaves all of your non-MS software unpatched, which in times when every average web malware exploitation kit is taking advantage of 10 to 15 different client-side vulnerabilities in the most popular video players, browsers, even browser plugins and widgets, doesn't speak for a good situational awareness on behalf of a bank

- The use of [free anti virus software is recommended](#) , next to using a third party anti spyware software. If you are aware of a spyware infection case through fully patched Firefox and Opera web

browsers point it out. There are exceptions with spyware coming in as a fake extension, but the fact that the emphasis in such an advice isn't on the recommendation of using another browser but IE, speak for itself from my perspective

- Encouraging the [use of the free ZoneAlarm](#) is not a bad advice compared to the opportunity for them to provide a benchmarked analysis of personal firewalls and which one scored the most based on the criteria the customer is interested in

And talking about the basics, the XSS vulnerabilities within the sites could have been detected even by the cheapest scanner out there. Most of them still remain active, let's see for how long.

How was Comcast.net hijacked? | ZDNet

It's official, even a pothead can social engineer Network Solutions. In [an in-depth interview with the hijackers](#) , featuring

some screenshots showing they had access to the complete portfolio of over 200 domain names controlled by Comcast, the details of how they did it, and why they did it are now coming straight from [the source of the attack](#) :

The hackers say the attack began Tuesday, when the pair used a combination of social engineering and a technical hack to get into Comcast's domain management console at Network Solutions. They declined to detail their technique, but said it relied on a flaw at the Virginia-based domain registrar. Network Solutions spokeswoman Susan Wade disputes the hackers' account. "We now know that it was nothing on our end," she says. "There was no breach in our system or social engineering situation on our end."

However they got in, the intrusion gave the pair control of over 200 domain names owned by Comcast. They changed the contact information for one of them, Comcast.net, to Defiant's e-mail address; for the street address, they used the "Dildo Room" at "69 Dick Tard Lane." Comcast, they said, noticed the administrative transfer and wrested back control, forcing the hackers to repeat the exploit to regain ownership of the domain. Then, they say, they contacted Comcast's original technical contact at his home number to tell him what they'd done.

Following ICANN's recently released advisory on [preventing the very same impersonation attacks](#) , it appears that even a first-tier domain registrar is still susceptible to registrant impersonation attacks. Makes you wonder on the state of understanding, detecting, and preventing social engineering attacks on the rest of the domain registrars.

How to remove the ICPP Copyright Violation Alert ransomware | ZDNet

Who would have thought that on your way to remove a ransomware scam that affected your PC, you would be one day pirating the application that was originally using a ["copyright violation alert" theme](#), as a spreading technique?

What's the best way of removing it? A working license code that completely uninstalls the ransomware, remains the most effective post-infection approach.

Although the original domain used to facilitate the \$400 transaction scam is down, a huge number of end users remain affected -- at least based on the few dozen of requests for removal instructions I received from Zero Day readers --despite the fact that the detection rate of the ransomware is relatively high - [iqmanager.exe](#) - Result: 35/41 (85.37%); [mm.exe](#) - Result: 29/41 (70.74%).

What would be the best, and most effective [way to get rid of the ransomware](#) once and for all, excluding the use of [freeware tools that detect and remove it](#) ?

It's by using the universal unlocking code/licensing code required in the *"Enter a previously purchased license code"* window. In this case that's **RFHM2-TPX47-YD6RT-H4KDM**

As always, [prevention](#) is better [than the cure](#) .

How to recover GPcode encrypted files? | ZDNet

Got backups? In response to the security community's comments on the futile attempt to directly [attack the 1024 bit RSA keys using distributed computing](#) , Kaspersky Labs [are now reasonably recommending](#) that affected end users lacking backups of their encrypted data, take advantage of data recovery tools :

Currently, it's not possible to decrypt files encrypted by Gpcode.ak without the

private key. However, there is a way in which encrypted files can be restored to their original condition. When encrypting files, Gpcode.ak creates a new file next to the file that it intends to encrypt. Gpcode writes the encrypted data from the original file data to this new file, and then deletes the original file.

It's known that it is possible to restore a deleted file as long as the data on disk has not been significantly modified. This is why, right from the beginning, we recommended users not to reboot their computers, but to contact us instead. We told users who contacted us to use a range of utilities to restore deleted files from disk. Unfortunately, nearly all the available utilities are shareware – we wanted to offer an effective, accessible utility that could help restore files that had been deleted by Gpcode. What did we settle on? An excellent free utility called PhotoRec, which was created by Christophe Grenier and which is distributed under General Public License (GPL).

Find out how to restore files encrypted by the GPcode ransomware by exploiting a weakness in the process in which the malware deletes the original files, why directly attacking the encryption algorithm was a futile attempt right from the very beginning, how would the malware authors adapt in the future and what can you do about it?

As I've already pointed out in a previous post "[Who's behind the GPcode ransomware?](#) " even through they've successfully

implemented the encryption algorithm this time, the only weakness in the process remains the fact that the malware authors are not securely deleting the original files, making them susceptible to recovery using data carving techniques, or through the use of plain simple point'n'click forensics software. If backups are not present, you would have to apply some marginal thinking given that not all of your affected files can be recovered, and therefore, recovering 500 out of 1000 is better than recovering none, isn't it? Whatever approach you take try to adapt to the situation, and don't pay. More info on [the Stopgpcode utility released by Kaspersky](#) :

To complete the recovery process, we've created a free utility called StopGpcode that will sort and rename your restored files. The utility will process the entire disk and compare the sizes of encrypted and recovered files. The program will use the file size as a basis for determining the original location and name of each recovered file. The utility will try to determine the correct name and location for each file, recreating your original folders and file names within a folder called "sorted". If the utility cannot determine the original file name, the file will be saved to a folder called "conflicted".

Next to the [step-by-step tutorial on using PhotoRec](#) , a data recovery utility, you can also [watch a video of the process](#) , or consider using [third-party data recovery utilities](#) next to their [web based alternatives](#) .

Why was the distributed cracking futile at the first place?

Mostly because the lack of easy to measure return on investment and applicability in a real-life situation - they could have simply started [using GPcode variants with new and stronger keys on a per variant basis](#) . The malware authors were also smart enough not to release a universal decryptor including the private key for all of their campaigns, instead, upon providing a custom built decryptor to the affected party, first they request the public key used in the encryption process to later one ship a customer tailored decryptor that works only for the encrypted files using the public key in question. Compared to the majority of malware variants attempting to infect as many hosts as possible, GPcode's currently targeted approach is willing to sacrifice some efficiency and emphasize on quality.

How would the malware authors adapt in the future?

[According to the author of Gpcode](#) , or the person responsible for processing the decryptor requests, new versions with stronger encryption are already in the works, including commodity malware features such as anti-sandboxing, polymorphism and self-propagating abilities. This would result in a awkward situation, for instance, for the time being two out of the four emails used by the authors of GPcode aren't even bothering to respond back to the infected party, so you can imagine the delays with responding given that GPcode starts self-propagating. They will basically end up with a situation where the number of affected people would outpace their capability to provide them with a custom built decryptor in a timely manner, even if someone's willing to pay the ransom.

With the entire GPcode ransomware fiasco slowly becoming a tool in the marketing arsenal of a backup company that can now use GPcode as a fear mongering tactic, [malware free backups](#) are once again [reminding us of their usefulness](#) .

How OpenDNS, PowerDNS and MaraDNS remained unaffected by the DNS cache poisoning vulnerability | ZDNet

The short answer is being paranoid about tackling a known vulnerability. It's **2001** , and [Daniel J. Bernstein \(DJB\)](#) ,

author of the then popular djbdns security-aware DNS implementation, is [applying basic math principles to raise awareness](#) on what's to turn into the "sky is falling" critical Internet vulnerability in **2008** , in an email on the unix.bind-users newsgroup :

"I said "cryptographic randomization." The output of random() is not cryptographically secure. In fact, it is quite easily predictable. This is a standard exercise in first-semester cryptography courses. Randomizing the port number makes a huge difference in the cost of a forgery for blind attackers---i.e., most attackers on the Internet. It's funny that the BIND company has gone to so much effort to move from the first line to the second, but now pooh-poohs the third line. Do you think that "RSA" is a magic word that makes security problems disappear? Without a central key distribution system---a system that doesn't exist now and won't exist for the foreseeable future---DNSSEC doesn't stop forgeries."

The skeleton from the closet [makes another appearance in January 2005](#) , according to **Marcus H. Sachs** , Director, SANS Internet Storm Center, in the face of [Ian Green's GIAC Security Essentials Certification \(GSEC\) submitted paper](#) detailing the same vulnerability :

"Three years ago Ian Green, then studying for his GIAC Security Essentials Certification (GSEC), submitted [a paper that details the same DNS spoofing vulnerability](#) , the SANS Institute's Internet Storm Centre notes. In order to spoof a DNS request it's necessary to "guess" both the Query ID and the source port. The query ID is 16 bits long, and the UDP source port also has over 60,000 potential options. But as Green noted back in January 2005, DNS transactions

are incremented by one for each subsequent query while the UDP source port remains the same during a session."

Apparently, OpenDNS, PowerDNS and MaraDNS were all aware of the possibility for abuse here, and took action long before the recent [vulnerability disclosure and coordinated multi-vendor patching initiated by Dan Kaminsky](#) took place. How did they do it, and what's the current state of the coordinated patching campaign across the Internet?

On July 8th, [David Ulevitch at OpenDNS posted a statement that OpenDNS isn't vulnerable](#) :

"I'm very proud to announce that **we are one of the only DNS vendor / service providers that was not vulnerable when this issue was first discovered by Dan** . During Dan's testing he confirmed (and we later confirmed) that our DNS implementation is not susceptible to the attack that was discovered. In other words, if you used OpenDNS then you were already protected long before this attack was even discovered.

In fact, for those of you who were listening in on the Microsoft press call this morning, you'll note that OpenDNS was suggested as the easy and simple solution for anyone who can't upgrade their DNS infrastructure today. Pointing your DNS servers to forward requests to OpenDNS and firewalling all other DNS traffic off at your server will help mitigate this risk." Bert Hubert, author of PowerDNS, alerted me to the fact that **PowerDNS was also not vulnerable when this issue was discovered** . That's not surprising considering Bert is one of the authors of the wonderful [DNS forgery resilience Internet Draft](#) that has recently been published. :-) I updated the statement in bold appropriately."

On July 9th, Sam Trenholme at MaraDNS pointed out that the service is too, [immune to the new cache poisoning attack](#) :

"MaraDNS is immune to the new cache poisoning attack. MaraDNS has always been immune to this attack. Ditto with Deadwood (indeed, people can use MaraDNS or Deadwood on the loopback interface to protect their machines from this attack). **OK, basically, this is an old problem DJB wrote about well over seven years ago. The solution is to randomize both the query ID**

and the source port ; MaraDNS/Deadwood do this (and have been doing this since around the time of their first public releases that could resolve DNS queries) using a cryptographically strong random number generator (MaraDNS uses an AES variant; Deadwood uses the 32-bit version of Radio Gatun)."

And while these DNS services and secure DNS implementations like MaraDNS in this case, weren't susceptible to the DNS

cache poisoning, during that time, across the Internet a synchronized patching was causing a lot of DNS anomalies, the direct effect of the ongoing patching in progress. [According to Narus's Supranamaya Ranjan](#) , they saw a 1000x increase in aggregate volume of anomalous DNS traffic between July 7th and 11th :

"Look at the figure below, which shows the aggregate volume (in Mbits/hour) over time for the DNS anomalies seen between July 7th and 11th. Clearly, before the CERT announcement and release of the patches, there were no anomalies. But after the announcement on July 8th, NSS saw a 1000x increase in aggregate volume of anomalous DNS traffic. NSS defines a traffic event as an anomaly if the amount or behavior of traffic heading to an ip-address exhibits sudden changes. A further analysis of the sources of these queries shows that they were being originated from open DNS proxies on the Internet and from DNS clients from well-reputed institutions from around the world. The reputation of the anomaly sources leads to the conclusion that these anomalies were not really attacks, but a side-effect of the synchronized patching."

The most [recent study on the state of patching vulnerable DNS servers](#) , was released today courtesy of Austria's CERT, stating that :

"The conclusions are rather grim so far – more than two thirds of the Austrian Internet's recursive DNS servers are unpatched while at the same time the upgrade adoption rate seems rather slow. Our findings are matched by the observations of Alexander Klink of Cynops GmbH who analyzed the results of the online vulnerability test on Dan Kaminsky's doxpara site."

The big picture? It seems that [it's not just At&T's DNS servers](#) which are susceptible to DNS cache poisoning, but [many other like the following](#) according to a [request for self-auditing](#) initiated by the Register :

"Skybroadband, Carphone Warehouse Broadband, Opal Telecom, T-Mobile, Videotron Telecom, Roadrunner, Orange, Enventis Telecom, Earthlink, Griffin Internet and Jazztel."

With **three publicly available exploits for remote DNS cache poisoning** released during the last three days "in the wild", it remains yet to be seen whether or not [malicious attackers would take advantage of the window of opportunity](#) , or continue using the "cybercrime as usual" attack tactics.

How many people fall victim to phishing attacks? | ZDNet

[According to](#) a recently released report, based on a sample of 3 million users collected over a period of 3 months, approximately [45% of the time, users submitted their login information to the phishing site](#) they visited.

The study, exclusively monitored users who successfully reached a live phishing site that was not blocked by their browser's built-in anti-phishing protection or filtered as fraudulent one ([Phishing experiment sneaks through all anti-spam filters](#)), and found out that on average, 12.5 out of one million customers sampled for a particular bank, visited the phishing site.

Here are some of the key findings from the report:

Each phishing attack compromises a very small number of customers (0.000564%), but due the large number of phishing attacks, the aggregated number is significant

45% of bank customers who are redirected to a phishing site divulge their personal credentials

0.47% of a bank's customers fall victim to Phishing attacks each year, which translates to between \$2.4M-\$9.4M in annual fraud losses (per one million online banking clients)

Each financial institution was targeted, on average, by 16 phishing websites per week

This translates to 832 phishing attacks per year per brand

The logic applied in the report is similar to the logic I once emphasized on in a previous post while disagreeing with claims made in another report on how unprofitable phishing, and underground economy are in general due to thousands of [cybercriminals stealing each other's market share of malicious activity](#).

It's simple math and a realistic "view from the trenches" perspective. For instance, if the price for launching a phishing campaign ([Spamming vendor launches managed spamming service](#)

) consisting of 50 million emails is \$500, if only a single user falls victim and loses \$501, the phisher breaks-even and earns profit.

Consider going through related posts: [Phishers introduce 'Chat-in-the-Middle' fraud tactic](#) ; [New study details the dynamics of successful phishing](#) ; [Research: 76% of phishing sites hosted on compromised servers](#) ; [Microsoft study debunks phishing profitability](#) ; [Microsoft study debunks profitability of the underground economy](#) ; [Phishers increasingly scamming other phishers](#) ; [DIY phishing kits introducing new features](#) ; [Phishers apply quality assurance, start validating credit card numbers](#) ; [Lack of phishing attacks data sharing puts \\$300M at stake annually](#).

[Trusteer's report](#) makes another interesting observation, and it's the fact that not only were the phishing sites live, but also, apparently managed to bypass the anti-spam/phishing protection -- if any -- on the potential victim's host.

With the average time for a phishing site to remain online varying based on multiple factors, what the industry and the security community in general can do to better [undermine this effectiveness of in-the-wild phishing attacks, is by sharing data](#) , ultimately protecting more people, a practice which according to research reports, can save up to \$300M annually.

The beneficial effects of data sharing were most recently confirmed in a [Virus Bulletin comparative review of anti-spam solutions](#) , in which [they concluded that](#) the "*combined effort outperformed individual products*":

"In the test, almost 200,000 emails were sent to 14 different anti-spam solutions which were required to classify them as either ham or spam. The test revealed that no legitimate mail was blocked by more than four products. After the test, VB's anti-spam team decided to look into this further and considered a hypothetical filter that marked an email as spam if at least five of the 14 products did so.

Unlike any of the individual products, the hypothetical filter generated no false positives at all, and combined this 0% false positive rate with an impressive overall spam catch rate of 99.89% (higher than any of the individual products VB has tested). "

Despite the [long term potential of phishing](#) , and the inevitable localization successfully reaching the native speakers of campaign's message, crimeware also known as banker malware such as [Zeus](#) , [Limbo](#) , [Adrenalin](#) or [URLZone](#), remain the financial industry's biggest enemies, bigger than any economic forecast, no matter how cloudy it is.

Be pragmatic and reclaim control of your bank account. [Bank on a LiveCD](#) , ask your bank about the daily withdrawal limit conditions and set them according to your needs, ask them about the [availability of SMS alert service](#) allowing you to receive real-time notifications for incoming and outgoing transactions as an early-warning system for bank account compromise.

Images courtesy of [PhishTank's Statistics](#) for November, 2009 and [Virus Bulletin](#) .

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/> and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back these settings

CLOSE

Plugins compromised in SquirrelMail's web server hack | ZDNet

According to a [recently posted update](#) by SquirrelMail's Jonathan Angliss, the source code of three plugins was backdoored during the web server compromise of the [popular web-based email application](#) which took place last month.

The compromised plugins were embedded with code that was forwarding accounting data to a server maintained by the people behind the hack, something SquirrelMail didn't acknowledge prior to [announcing the web server compromise](#) .

During the initial announcement, we'd mentioned that we did not believe that any of the plugins had been compromised. Further investigation has shown that the following plugins were indeed compromised: - sasql-3.2.0 - multilogin-2.4-1.2.9 - change_pass-3.0-1.4.0

Parts of these code changes attempts to send mail to an offsite server containing passwords.

SquirrelMail has a total of 222 plugins available in 14 categories. Its [SourceForge repository](#) was not affected.

'Pixmania.com payment order detail' themed emails serving SpyEye crimeware | ZDNet

Security researchers from "[Stop Malvertising Spam & Scams](#)", have [intercepted a currently circulating malicious email campaign](#), that's impersonating GestPay, and is spreading using '*Pixmania.com payment order detail*' subjects.

The campaign is carrying the following malicious attachment **informazioni.zip**, which includes the **informazioni.scr** bogus screensaver found inside the archive. Upon execution, the bogus screensaver will phone back to download a copy of the SpyEye crimeware from **hxxp://mybackdomain888.in/balance/index.php**.

End and corporate users are advised to avoid interacting with the emails, and to immediately report them as spam/fraudulent in order to help protect millions of other users.

'Photographer committed SUICIDE 3 days after shooting THIS video!' scam spreading on Facebook | ZDNet

A currently spreading Facebook scam, is enticing end users into clicking on a virally spreading fake video link.

Upon clicking on the link, the user is exposed to a fake Facebook screen, and is being asked to double click on the "Jaa" link in order to pass a bogus age verification test.

Once the user clicks on the link, he or she will spread a link to the bogus video on their wall, further assisting the propagation of the scam.

Users are advised to pay extra attention to such virally spreading Facebook scams, and avoid interacting with them.

Photobucket's DNS records hijacked by Turkish hacking group | ZDNet

Yesterday, [Photobucket](#) the world's most popular photo sharing site [according to Hitwise](#) had its DNS records hijacked

to return a hacked page courtesy of the [NetDevilz hacking group](#) , a Turkish web site defacement group most widely known for its defacement of the [adult video site Redtube](#) earlier this year. Photobucket users across the world are reporting minor outages of the service and problems when trying to access their accounts, the consequence of what looks like the type of DNS records hijacking that [redirected Comcast.net to a third-party domain](#) last month.

Third-party site monitoring services indicate that the site was down for 15 minutes yesterday, from from 17:39:39 to 17:55:10, whereas according to a comment left by a [Photobucket Forum Support representative](#) , the downtime due to the propagation of the corrected DNS entries was longer :

"On Tuesday afternoon, some users that typed in the Photobucket.com URL were temporarily redirected to an incorrect page due to an error in our DNS hosting services. The error was fixed within an hour of its discovery, but due to the nature of the problem, some users will not have access to Photobucket for a few hours as the fix rolls out. It is important to note that only a portion of Photobucket users encountered the problem and that no Photobucket content, password information or other personal information was affected by the redirect."

The NetDevilz hacking group left the following message, that appears to have been loading from a third-party domain,

atspace.com in this case :

"... ve NeTDevilz yeniden sahnede

Bizi hat?rlayan var m? ? Unutuldu?umuzü dü?ündük ve tekrar hat?rlatmaya karar verdik ! (Turkish hackers group)

ZeberuS - GeCeCi - MiLaNo - The_BeKiR - h4ckinger - SerSaK - KinSize

we are came back ! ©2008 NetDevilz Co. We're not first,But We're the BEST!"

The hacking group appears to have been using the [hosting services of atspace.com](#) , the web hosting service of Zetta hosting solutions, and users of Photobucket attempting to access the site with the old DNS entries are still being redirected to a [default hosting ad page within atspace.com](#) . The effect of the redirection can also be seen by taking a peek at the publicly obtainable [stats for atspace.com](#) , where the sudden peak in traffic resulting in 118,864 visitors for today came from the default ad page used in the redirection.

With the second DNS hijacking attack against a high-profile domain in the recent months, it seems that adaptive malicious parties unable to directly compromise a site will continue taking advantage of good old-fashioned DNS hijacking. At least to prove that it's still possible even on a high-profile domain using the services of a Tier 1 domain registrar.

Phoenix Mars Lander's mission site hacked | ZDNet

With the world's eyes on the latest multimedia streaming straight from Mars, during the weekend [the Phoenix Mars](#)

Mission's site got hit twice, first by an Ukrainian web site defacer who posted a message at the site's blog, and hours later, the Turkish "sql loverz crew 2008" [redirected the official mission's site](#) , as well as the [Lunar and Planetary Laboratory](#) site to a third-part location serving the defaced page. The Phoenix Mars Lander mission's security staff are aware of the issue, and seem to have fixed it already, right before making an announcement - [Hacker changes Phoenix Mars Lander Web site](#)

A spokeswoman for the Phoenix Mars Lander mission says a hacker took over the mission's public Web site during the night and changed its lead news story. Spokeswoman Sara Hammond says a mission update posted Friday was replaced with a hacker's signature and a link redirecting visitors to an overseas Web site. Hammond says the site hosted by the University of Arizona has been taken off line while computer experts work to correct the problem.

Meet the latest group of script kiddies empowered by publicly obtainable remote SQL injection scanners, that each and

every site that's been affected in the past could have downloaded, and self-audited itself. The perspective that if you don't take care of your site's web application vulnerabilities, someone else would, fully applies here. No malware, or false information was distributed despite that the defacer linked to what looks like his homepage and therefore could have embedded malicious links or directly pointed the surfer to them.

And while this doesn't seem to be what they wanted to achieve, in three of the most recent web site defacement incidents, we have defacers fully abusing the access they have. Last month for instance, [Russian nuclear power websites were attacked and nuclear accident rumors spread using them](#) , the [Pro-Serbian](#)

[hacktivists attacking Albanian web sites to spread propaganda messages](#) , as well as a [fake rumor for upcoming earthquake](#) spread on the site of a Chinese seismological bureau.

Phishing experiment sneaks through all anti-spam filters | ZDNet

A recently conducted ethical phishing ([New study details the dynamics of successful phishing](#)) experiment impersonating LinkedIn by mailing invitations coming from Bill Gates, has achieved [a 100% success rate in bypassing the anti-spam filters](#) it was tested against.

The experiment emphasizes on how small-scale spear phishing campaigns are capable of bypassing anti-spam filters, and once again proves that users continue [interacting with phishing emails](#).

More info on the methodology used:

"This scenario was an invitation from LinkedIn, posing as an invitation from Bill Gates to join his network. LinkedIn was selected due to availability, and the fact that it is a social network recognized by most executives. This selection of LinkedIn was also based on the fact that linked-in email should be already identified by most existing email system(s), and this may have helped delivery through into the mailbox. The phishing link can be identified in the HTML source code below.

The Phishing site was based on the LinkedIn sign in page. The form action was changed so that the user would be redirected to a subsequent page on our site. No usernames or passwords were collected during this assessment. All targeted users were contacted before the phishing email was sent, and were expecting a LinkedIn invitation from Bill Gates."

A similar study was conducted by ethical phishing vendor **PhishMe.com** in March this year, pointing out that based on the [32 phishing scenarios tested against 69,000 employees](#), people are less cautious when clicking on active links in emails than when they are requested for sensitive data. This behavior is not surprisingly cited by **PhishCamp** as a possible opportunity for the introducing of blended threats, similar to known cases where [phishing](#) and [scareware](#) sites were also serving [client-side exploits](#).

Go through related posts: [419 scammers using Dilbert.com](#) ; [419 scammers using NYTimes.com 'email this feature'](#) ; [Fortune 500 companies use of email spoofing countermeasures declining](#) ; [Gmail, Yahoo and Hotmail systematically abused by spammers](#)

With the average price for a thousand active Gmail, Yahoo Mail and Hotmail accounts decreasing due to the economies of scale achieved by the vendors of CAPTCHA-solving services, and the numerous tools available at the spammer's disposal to take advantage of these accounts, in the long-term all spammers will start [abusing the already established DomainKeys trust](#) among the most popular free email service providers.

What's the success rate of spam and phishing emails hitting your inbox? What about your corporate email? Also, do you believe that ethical phishing is most constructive way of building awareness on phishing attacks, or do you think that it drives innovation in the wrong direction by attempting to gather click-through metrics instead of advising users to avoid interacting with such emails in general?

TalkBack.

Phishers targeting Facebook users, fake logins spammed through hacked accounts | ZDNet

A currently [active phishing campaign](#) is circulating across Facebook end users' walls, using already compromised accounts to post the phishing links, tricking the user into thinking it's a legitimate friend sending the message in order to redirect them to a fake login page. The campaign is taking advantage of multiple typosquatted domains which are in a fast-flux state, namely, they respond to multiple IP addresses and change them automatically every three minutes in this particular attack.

Sample phishing URLs used look like the following :

facebook.com.profile.id.ep7vu2.749e92q.**916ad771.info**
facebook.com.profile.id.mgt9fr5n.mg6qdo.**e77c98037.com**
facebook.com.profile.id.bvbu38.krpz.**dortos.net**
facebook.com.profile.id.10g10th3.7q342k8.**31dd6db6.com**

This is not the first, and definitely not the last time Facebook's been under attack by phishers and malware authors. For instance, at the beginning of the year, a [malware serving phishing attack](#) that was originally [targeting MySpace](#) , switched to [Facebook](#) "in between" two months later. What's "the instant nature of social networking" to some, is real-time spamming capabilities to others, who based on the number of accounts hacked, would be able to efficiently spam any social network.

Sometimes, your hacked friends are not to be trusted but warned, so that they get the chance to change their passwords and no longer participate in phishing attacks through their accounts.

Phishers introduce 'Chat-in-the-Middle' fraud tactic | ZDNet

Phishers don't just want to "bank with you", they also want to talk you into revealing the answers to your 'secret' questions, next to more sensitive information that would help them gain access to your online bank account.

A new '[Chat-in-the-Middle' fraud tactic](#) was recently discovered by the **RSA FraudAction Research Lab**, according to which the phishing site intercepted is using the hosting services of a well known managed cybercrime network, with the campaign itself in an apparent test mode since they've only detected a single instance of the attack.

Here's how it works, and why going mainstream with such a feature from a phisher's perspective may in fact [make their phishing campaign a less profitable, and much more time-consuming process](#) than it currently is:

Basically, the prospective victim receives a phishing email detailing a compromise at the targeted financial institution or request for personal data confirmation, requiring them to enter their authentication details and personal identification on a phishing site. Once the prospective victims visit the site, a Live Chat box pops-up with a "phishing assistant" attempting to walk you through the process of having your bank account compromised:

Through social engineering, the fraudster attempts to obtain further information from the victim over the live chat platform. The fraudster presents himself as a representative of the bank's fraud department, claiming that the bank is "now requiring each member to validate their accounts". The fraudsters then collect additional information pertaining to the user - name, phone number and email address. These details may facilitate online or phone fraud against the user's account, and are possibly used for contacting the customer at a later stage as suggested in the chat window.

Certain phishing gangs are known to understand the basics of quality assurance in the past, with the majority of their [DIY \(do-it-yourself\) phishing pages](#) coming with [built-in credit card validation checks](#) in order to ensure that no bogus financial will be submitted, thereby requiring time and resources to sort out the real phished data. In this sense, is the newly introduced 'Chat-in-the-Middle' fraud tactic yet another featured released with quality assurance in mind, or is it an experiment whose lack of efficiency-oriented approach common for cybercriminals will spell its demise?

In terms of Q&A the resources and money required to maintain such "Live phishing representatives" outpace the "benefits" of localization -- still largely under-developed -- which would apply basic [market segmentation approaches combined with translated phishing pages](#) to the native language of the prospective victim.

Underground social engineering services on demand have been available for years. Last year, a newly launched such service was offering "[social engineering services over the phone](#) " doing exactly what the people behind the 'Chat-in-the-Middle' are attempting to do. The service is offering male and female voices in five different languages, and is charging \$9 per call, appears to have been launched in order to break the language barrier for cybercriminals.

However, if a mainstream phishing gang using mass marketing practices and not relying on targeted attacks were to implement a Live Chat and a "phishing campaign assistant", it would undermine one of their key success factors - the volume of the campaign and the millions of emails sent where even if a small number of victims get phished it would still mean a profit for them. A profit they would have to share with the "Live phishers".

Phishing stats graph courtesy of [Symantec's August Spam Report](#)

Phishers increasingly scamming other phishers | ZDNet

A new study conducted by [Marco Cova, Christopher Kruegel, and Giovanni Vigna](#) , provides factual evidence of a well

known practice by experienced phishers, namely, backdooring phishing pages that they would later on distribute for free across the IT underground, in order to build a covert network where other phishers would be unknowingly providing them with the accounting data that they would eventually obtain :

"We consider a kit to be backdoored if it sends the phished information to addresses other than those found in clear in the kit's code. **We found 129 of the kits from distribution sites (slightly more than one third) to be backdoored. Among live kits, 61 (40%) are backdoored. Of these, 20 send the phished information to addresses also found in 8 kits obtained from distribution sites.** Assuming that authors and users of kits are different individuals, this shows that backdoors are effective. That is, in a significant number of cases, they do not appear to be detected. At the same time, it seems that, when identified, backdoors are updated to send the stolen information to new recipients."

Backdooring phishing pages is a rather primitive example of cybercriminals attempting to scam other cybercriminals. Moreover, [a distinction should be made between a phishing kit and phishing page](#) in order to consider the minimalistic impact of backdooring a single phishing page, or an entire phishing kit, where the second approach would aim at obtaining all of the stolen virtual goods on the second cybercriminal's computer if he's naive enough to get infected with a phishing kit that would ironically let another cybercriminal get hold of all the virtual goods he has already stolen.

The more sophisticated tactics have to do with attempts to hijack one another's botnet though [exploiting remotely executable flaws in popular malware kits, like Zeus and Pinch for instance](#) , both of which are vulnerable flaws allowing someone to backdoor the

command and control interfaces. Crimeware just like legitimate software is vulnerable to insecure coding practices, which when combined with [the obvious monopoly of a certain crimeware kit](#) easily puts it under a coordinated code scrutiny from the IT underground, looking for ways to [exploit access to known command and control servers](#) . Now, that's a far more "beneficial" approach of scamming one another next to simply backdooring a phishing page, since crimeware kits serving [banking malware use far more sophisticated approaches to hijack E-banking sessions](#) , compared to a simple phishing email.

Taking a more strategic approach, a cybercriminal wanting to scam another cybercriminal would backdoor [a highly expensive web malware exploitation kit](#) , then start distributing it for free, and in fact, there have been numerous cases when such kits have been distributed in such a fraudulent manner. The result is a total outsourcing of the process of coming up with ways to infect hundreds of thousands of users through client side exploits [embedded or SQL injected at legitimate sites](#) , and basically collecting the final output - the stolen E-banking data and the botnet itself.

Ironically, there's no such thing as a free web malware exploitation kit if we're to consider the existence of backdoored kits, and with cybercriminals starting to realize the return on investment of having someone else to do the scam for them, knowingly or unknowingly, we'll be definitely witnessing more activity in the spirit of cybercriminals attempting to scam other cybercriminals.

Phishers apply quality assurance, start validating credit card numbers | ZDNet

With the exact number of end users interacting with phishing emails by submitting bogus data still unknown, phishers are on the other hand continuing to apply basic quality assurance processes ensuring that they will be collecting only validated credit card details, and limiting the opportunity for [researchers and end users to poison their campaigns](#) .

For instance, a recent blog post at Symantec's Security Response blog analyzes a phishing page where [the fraudster is applying credit card validation checks](#) before accepting anything, an approach that in times when [phishers are attempting to scam other phishers](#) , can easily turn into a commodity feature for phishing pages in general -- even the backdoored ones.

"Fraudsters are aware of these techniques and are continuously trying to optimize their attacks and thus their profits. As a proof of concept, shown below is a piece of PHP code revealed from a phishing attack that is intended to check the validity of the credit card number provided by the user according to card number conventions. After performing this check, the fraudster tries validating the card number by using the Luhn algorithm (figure 2). If both conditions are met (the card number appears to be correct and the Luhn algorithm is verified) the information is delivered to the drop box. This approach makes the Random Data Dilution strategy described above useless, because invalid data won't be accepted. The piece of code in figure 3 (below) shows one of these tricks, which checks to see if the credentials provided by the user are indeed valid. It has been implemented by submitting the credentials to the original website and then identifying specific patterns in the response page in order to verify their validity."

The phishers in this particular case are capable of achieving the validation by forwarding the submitted data to the original site, potentially exposing their campaigns in the process, if only was the

targeted company properly monitoring where traffic is coming from. Phishers tend to switch tactics or introduce new ones on a quarterly basis, and with [EstDomains about to face the music](#) , yesterday Sophos already started detecting [phishing campaigns targeting exclusively domain registrants](#) by impersonating eNom and Network Solutions. Despite the potential for abuse of legitimate domains once the domain portfolio owner falls victim into the phishing scam, data mining malware infected hosts for domain registrant's accounting data seems to be the tactic of choice on a large scale, at least for the time being.

Poisoning a phishing campaign by submitting bogus data or personal messages to the phisher isn't the way. If you truly want to express your feelings about a phisher - report their campaigns.

Image courtesy of the [Anti-Phishing Phil](#) .

Pfizer's Facebook hacked by AntiSec | ZDNet

According to a screen post published by the [Script Kiddies group](#), the world's largest pharmaceutical company has had [its Facebook page](#) hacked last week. Once the group gained access to the account, they posted numerous messages on Pfizer's wall:

“The guy in charge of this Facebook. Hint for next time: protect this company with a LITTLE better security. One Google search and I’m in.”

Pfizer's Facebook account is now restored back to normal.

Paul McCartney's official site serving malware | ZDNet

All you (don't) need is malware on Paul McCartney's official web site.

[According to Mary Landesman at ScanSafe](#) , the official web site of Paul McCartney (paulmccartney.com) has been compromised, and is serving live exploits to its visitors. Landesman points out that the compromise might have occurred through stolen FTP accounting data, taking into consideration the fact that the campaign is also present at several different flat HTML only web sites.

The process of automatically [injecting malicious code at hundreds of sites through compromised FTP accounts](#) is nothing new, and continues being in a development phase with [the most recent kit](#) released earlier this year. What has changed through, is the typical proposition for bulk-orders of data mined FTP credentials from botnets which the sellers are now offering to bargain hunters of such tools.

Go through related incidents - [Paris Hilton's official web site serving malware](#) ; [eBay solutions provider Auctiva.com infected with malware](#) ; [USAID.gov compromised, malware and exploits served](#) ; [Adobe's Serious Magic site SQL Injected by Asprox botnet](#) ; [200,000 sites spreading web malware, China's hosting the most](#) ; [Sony PlayStation's site SQL injected, redirecting to rogue security software](#) ; [Redmond Magazine Successfully SQL Injected by Chinese Hacktivists](#)

Here's a brief analysis of Paul McCartney's site compromise. The attack is taking advantage of a newly distributed web malware exploitation kit which is already gaining popularity across the cybercrime ecosystem due to the several new features, among which is the use of RSA encryption of the javascript. Upon several redirections (**84.244 .138.55 /google-analytics/ga.js -> 84.244 .138.55 /ts/in.cgi?sliframe -> 84.244 .138.55 /ase/?t=17**), the

visitor is exposed to the typical set of already patched client-side vulnerabilities which vary based on the administrator's preferences.

The bottom line - would efficient exploitation of stolen FTP account data obtained through data mining an infected set of hosts re-emerge as a tactic of choice, or would massive SQL injection attacks through search engines reconnaissance targeting everyone, everywhere continue being the method of choice? In an increasingly multitasking cybercrime ecosystem, a combination of tactics is usually the method of choice.

Password stealing malware masquerades as Firefox add-on | ZDNet

Malware [researchers at BitDefender](#) are reporting on a newly discovered malware ([Trojan.PWS.ChromeInject.B](#)) that when once dropped in Firefox's add-ons directory starts operating as such, and attempts to steal accounting data from a predefined list of over a hundred E-banking sites. Once the accounting data is obtained, it's forwarded to a free web space hosting provider in Russia. Earlier this year, a more severe incident took place when the [Vietnamese Language Pack](#) hosted at Mozilla's official list was [infected with malware](#) .

"It drops an executable file (which is a Firefox 3 plugin) and a JavaScript file (detected by Bitdefender as: Trojan.PWS.ChromeInject.A) into the Firefox plugins and chrome folders respectively. It filters the URLs within the Mozilla Firefox browser and whenever encounter the following addresses opened in the Firefox browser it captures the login credentials. It is the first malware that targets Firefox. The filtering is done by a JavaScript file running in Firefox's chrome environment."

Despite the novel approach used, the malware would have made a huge impact if it were released several years ago when E-banking authentication was still in its infancy since plain simple keylogging is one part of the session hijacking tactics used. And while they will indeed obtain the accounting data, this is no longer sufficient for a successful compromise of a bank account. In comparison, the techniques used by sophisticated crimeware like Zeus, [Sinowal](#) and Wsnpoem [undermine the majority](#) of two-factor [authentication mechanisms](#) used by [E-banking providers](#) , since once you start doing E-banking from a compromised environment nothing's really what it seems to be anymore.

Paris Hilton's official web site serving malware | ZDNet

The official web site of Paris Hilton (**parishilton.com**) has been embedded with a malicious iFrame, automatically exposing visitors to client-side vulnerabilities and banker malware, according to researchers from [ScanSafe](#). Upon closer analysis, it appears that the site has been infected on the 8th of January, Thursday, becoming the very latest legitimate site whose use of outdated web application software led to its exploitation.

Moreover, just like we've seen in previous related attacks, Hilton's site compromise is a part of bigger malware campaign affecting several thousand sites, and is not being exclusively targeted.

A javascript embedded at the bottom of the site, is actually an iFrame that used to point to the now down **you69tube.com/flvideo/.a/.t/index.php**. Once the downloader is executed it attempts to download another binary from the same site, including configuration files from several other sites among which is **ManggaTv.com**. The abuse and use of legitimate infrastructure as a foundation for the entire malicious campaign, is a common practice applied by cybercriminals these days. For instance, in this campaign not only is the official web site of a popular celebrity used to acquire the traffic, but also, another legitimate site is used as a dropzone for the configuration file of the banker malware.

Go through related incidents - [Adobe's Serious Magic site SQL Injected by Asprox botnet](#) ; [200,000 sites spreading web malware, China's hosting the most](#) ; [Sony PlayStation's site SQL injected, redirecting to rogue security software](#) ; [Redmond Magazine Successfully SQL Injected by Chinese Hacktivists](#) ; [Over 1.5 million pages affected by the recent SQL injection attacks](#).

Let's discuss the attackers' logic applied here. [December's massive SQL injection](#) attack affecting thousands of Chinese web sites used as infection vectors serving the IE XML parsing zero day, is an example of the "long tail of SQL injected sites" versus targeted

attacks against high profile sites. Basically, their mentality relies on the fact that not only would thousands of sites acquire more traffic than a high profile one, but also, that their campaign may live longer if they diversify instead of centralizing it by using a single high profile site despite the anticipated traffic that would come from it.

For the time being the malicious iFrame has been removed, and the malware campaign is in a cover-up phrase -- they wish.

Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown | ZDNet

Following last week's [shutdown of 3FN/Pricewert's operations by the FTC](#), wishful thinkers expected a major decline in the overall spam volume, with botnet masters once again caught off guard just like it happened in [November, 2008 with McColo's shutdown](#).

However, according to numerous vendors that [doesn't seem to be the case](#). The short-lived 15% drop in spam volume quickly returned to its usual proportions, with only two of the big botnets (Pushdo/Cutwail along with Mega-D) affected for the time being.

Here's what the vendors and their data is saying:

According to managed e-mail and web security services [vendor MX Logic](#), the 3FN/Pricewert shutdown "*spam volumes haven't been affected at all*" according to data from their [Threat Operations Center](#), where the minor decline is pretty visible, prior to FTC's press release on the 4th of June.

The company attributes the lack of visible affect on the overall spam volume due to the contingency planning applied by the botnet masters, as well as the lack of more effective cooperation with the increasingly decentralized domain registrars increasing the average time a malicious domains remains online.

This decentralization has in fact allowed cybercriminals to centralize their bulk malicious domain registration process at cybercrime-friendly registrars such as EstDomains ([Cybercrime friendly EstDomains loses ICANN registrar accreditation](#); [ICANN terminates EstDomains, Directi takes over 280k domains - Q&A with ICANN's Stacy Burnette](#)).

Marshal8e6's [TRACElabs team](#) points out that "*looking at our Spam Statistics from last week, we do see a dip down of about 15% in our Spam Volume Index (SVI), and spam originating from the Pushdo botnet indeed seems to be affected. The proportion of spam from Pushdo has dipped, along with Mega-D. Rustock seems completely unaffected.*"

On the very same day the affected [Pushdo botnet spammed](#) a fake greeting card in an attempt to distribute the Privacy Center scareware, in an apparent attempt to signal its existence.

This modest decline can also be seen through daily spam data obtained from [Cisco IronPort's SenderBase](#) , with the global spam volume clearly declining June 5th with -8% fluctuation, followed by another -22% decline on the 6th. However, the daily volume then quickly returned to its usual rate.

Proofpoint [describes the post-shutdown effect](#) of 3FN/Pricewert on spam as "minimal", in comparison to the [shutdown of McColo](#) last year.

It should also be noted that [cyber-crime friendly ISPs have feelings](#) too, [just like cybercriminals do](#) as a matter of fact :

"At first, our technicians thought something was going wrong," said Christopher, about the sudden shutdown. He said the FTC "has ruined our reputation" and has caused loss of customers. Christopher, who says he is from Ukraine, added that he hopes the firm isn't being targeted because it has associations with Ukraine, which has gotten a bad reputation in some circles for malware distribution and online crime."

The firm is targeted due to its evident connections with key botnets and malware attacks, however, it appears that several [ICQ chats obtained by the FTC](#) offered a pretty descriptive insight into the customer relationship management practices offered by 3FN/Pricewert:

"In one of the chats obtained by the FTC, Pricewert's Head of Programming is engaged in a conversation with a customer regarding the number of compromised computers the customer controls. The customer informs Pricewert that he controls 200,000 bots and needs assistance configuring the botnet. The head of Pricewert's Programming Department agrees to assist, but complains upon learning of the size of the botnet that it will require a lot of work. In a second chat, a Senior Project Manager for Pricewert is told by a customer that the customer controls a massive and rapidly growing network of bots. Pricewert's Sales Director reassures the customer that "Well, we know how to manage it."

History repeats itself. October, [2008's disconnection of California based Atrivo/Intercage](#) once again briefly disrupted spam levels. However, a month later, the single most [successful disruption of a rogue ISP](#) in the face of McColo, seems to have taught the botnet masters a simple lesson - don't put all your eggs in a single basket, as well as the basics of contingency planning.

With several U.S based exceptions such as for instance [Layered Technologies](#) where Rustock was running for cover following the shutdown of McColo (the company has been the de-facto hosting provider for a [botnet for hire](#) service operating for several years, among other activities), the majority of the the [cybercrime-friendly ISPs are based outside the U.S](#) , and remain the hardcore cybercriminal's hosting provider of choice.

Over a million web sites affected in mass SQL injection attack | ZDNet

[Security researchers](#) from Armorize have intercepted a [mass SQL injection attack](#), targeting ASP ASP.NET websites.

The mass infection, redirects users to a web malware exploitation kit, attempting to exploit vulnerabilities in [Adobe PDF](#) or [Adobe Flash](#) or [Java](#), with the dropped malware having a [low detection rate](#).

Mass SQL injection attacks usually take place through active search engines reconnaissance ([SQL Injection Through Search Engines Reconnaissance](#); [Massive SQL Injections Through Search Engine's Reconnaissance - Part Two](#); [Massive SQL Injection Attacks - the Chinese Way](#)) followed by automatic exploitation of the vulnerable sites.

Of the two SQL injected domains **nbnjkl.com** and **jjghui.com**, only **nbnjkl.com** is currently active and responding. The campaign is directly related to the [Lizamoon mass SQL injection attacks](#), as the same email that's been used to register [Lizamoon domains](#) is currently used to register **nbnjkl.com** and **jjghui.com**.

Users are advised to take advantage of [NoScript](#) in order to protect themselves from this, and many other Web based threats.

Over 1.5 million pages affected by the recent SQL injection attacks | ZDNet

In an attempt to mitigate the impact of the recent waves of SQL injection attacks, and provide more transparency into the approximate number of affected pages, the Shadowserver Foundation is starting to maintain a list of all the

malicious domains used in the continuing efforts by copycats to inject as many legitimate sites as possible. Currently counting over fifty malicious domains, and the corresponding number of affected pages by them, the total number is just over 1.5 million.

Needless to say to stay away from these domains if you don't know what you're doing. [The Shadowserver's announcement](#) :

"Below is a list of domains used in the mass SQL injections that insert malicious javascript into websites. We've also included an approximate number of pages infected (according to Google). Note that these numbers decay with time. Some of these domains were injected long ago and have been cleaned. At their height, their numbers may have been larger."

Despite that some of the malicious domains are down, or in a process of getting shut down, as long as the long tail of SQL injection attacks is possible due to vulnerable sites at the far corner of the Web, the bad guys would simple keep re-introducing new domains within, or emphasize on [increasing their life cycle by fast-fluxing them](#) as we've already seen this happen.

Osama execution video scam spreading on Facebook | ZDNet

Multiple users are falling victims into a fast-spreading Facebook scam, using the "*Osama EXECUTION video* " theme.

Upon clicking on the tiny.cc shortened URL -- described as *Special Forces hit squad put a bullet in the head of Bin Laden!* -- users are asked to copy and paste a tiny javascript code into their browsers in order to reveal the video. By doing so, they will automatically post a link of the spreading instructions on the walls of their friends.

There's no actual video to look at, which could naturally change at any given moment of time, to include something more malicious rather than the spreading mechanism itself.

There are currently over 4.266 users at the scam site. Users are advised to avoid interacting with the propagating mechanism and report the site as a fraudulent one.

OS fingerprinting Apple's iPhone 2.0 software - a "trivial joke" | ZDNet

Just like every decent web service out there wanting to identify the iPhone's mobile Safari browser in order to serve

custom applications, in this very same way malicious attackers would like to remotely identify iPhone devices through a basic pen-testing practice known as [OS detection or OS fingerprinting](#) . It seems that the difficulty level of [identifying an iPhone device using nmap's](#) criteria is a "trivial joke", namely, it's too easy to accomplish :

"So, nmap 4.60 is accurately identifying the iPhone 2.0 software as an "Apple iPhone mobile phone or iPod Touch audio player". And that's by using its single open TCP port — 62078. First, it's reporting my last reboot as being Fri Oct 27 22:04:38 2006, which is highly incorrect. Even more interestingly, nmap is claiming that the sequence number prediction on the open port is weak (a trivial joke, as it were). That's kind of 80'sish, so I didn't believe it until I confirmed this via multiple connections to the port. Yep, definitely some weak ISN sauce. I'll have to research what that service is later. Anyway, here's the scan result."

With mobile phone providers dedicating special and sometimes too obvious netblocks for mobile users, [default iPhone passwords assisting automated attacks](#) through OpenSSH installed, next to the increasing number of [customers jailbreaking](#) and taking advantage of ([insecure and misconfigured](#)) third-party applications including those who would take advantage of [tethering their iPhone's 3G connectivity for their laptops](#) , the possibilities for building hit lists to use in [remote code execution](#) attacks through already identified devices is easier than it should be.

Opera for Mac OS X patches six security vulnerabilities | ZDNet

The latest version of the Opera browser for Mac OS X, [patches six security vulnerabilities](#), some of which could allow execution of arbitrary code on the affected machines.

More details on the vulnerabilities:

- [Fixed an issue](#) that could cause Opera not to correctly check for certificate revocation
- [Fixed an issue](#) where CORS requests could incorrectly retrieve contents of cross origin pages
- [Fixed an issue](#) where data URIs could be used to facilitate Cross-Site Scripting
- Fixed a high severity issue, as reported by Gareth Heyes
- [Fixed an issue](#) where specially crafted SVG images could allow execution of arbitrary code, as reported by Attila Suszter
- [Fixed an issue](#) where specially crafted WebP images could be used to disclose random chunks of memory, as reported by the Google Security Group

Users are advised to upgrade to the latest version immediately.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Opera for Mac OS X patches 6 security holes

| ZDNet

The [Opera Web browser for Mac OS X](#) has been recently updated to version 11.62, with the latest update patching six security holes.

Details on the fixed vulnerabilities:

Fixed an issue where small windows could be used to trick users into executing downloads, as reported by Jordi Chancel; see our [advisory](#). Fixed an issue where overlapping content could trick users into executing downloads, as reported by Jordi Chancel; see our [advisory](#). Fixed an issue which could allow web page content to overlap the address field; see our [advisory](#). Fixed an issue where history.state could leak the state data from cross domain pages; see our [advisory](#). Fixed an issue which could allow web page dialogs to display the wrong address in the address field; see our [advisory](#). Fixed an issue where carefully timed reloads and redirects could spoof the address field, as reported by Jordi Chancel; see our [advisory](#).

Users are advised to update to the latest versions immediately, either through the browser's built-in updater, or directly download the latest version from [Opera's web site](#).

Open source software security improving | ZDNet

You cannot say something's good or bad unless you benchmark or compare it against something else. According to the

[Linus's Law](#) , "given enough eyeballs, all bugs are shallow", a mentality which when combined with static code analysis of the most popular and widely used open source projects such as Firefox, Linux and PHP and benchmark it against 250 other open source projects, can truly make an impact. Is open source software security improving? [Coverity's](#) recently released [Open Source Report 2008](#) , indicates it is.

Key summary findings of the report :

Findings are based on analysis of over 55 million lines of code on a recurring basis from more than 250 open source projects, representing 14,238 individual project analysis runs for a total of nearly 10 billion lines of code analyzed. In summary, this report contains the following findings:

- The overall quality and security of open source software is improving – Researchers at the Scan site observed a 16% reduction in static analysis defect density over the past two years
- Prevalence of individual defect types – There is a clear distinction between common and uncommon defect types across open source projects
- Code base size and static analysis defect count – Research found a strong, linear relationship between these two variables
- Function length and static analysis defect density – Research indicates static analysis defect density and function length are statistically uncorrelated
- Cyclomatic complexity and Halstead effort – Research indicates these two measures of code complexity are significantly correlated to codebase size

- False positive results – To date, the rate of false positives identified in the Scan databases averages below 14%

The most prevalent defect found in the study was the [null-pointer dereference](#) representing 27.95% of all defects, followed by resource leak, and the most commonly known buffer overflows comprising only 6% of the total issues identified. Perhaps the most valuable benefit out of the whole project is the fact that insecure coding practices would be easily spotted, and more awareness build on [how to prevent this from happening](#) . Consider going through the report, and [include your open source software in the Scan project](#) .

Online broker CommSec criticised for weak passwords, lack of SSL | ZDNet

In times when vendors are vertically integrating by offering [virtual keyboards for secure Ebanking](#) , and banks themselves are [requiring end users to run antivirus software](#) if they were to file a fraud claim, others are busy [fixing security design flaws](#) .

Earlier this month, a Melbourne based computer programmer discovered that the 1.7m customers of Australia's largest online broker CommSec, have been using the site's services through outdated password best practices, providing them with the option to use a basic numeric password, which is logically increasing the potential effectiveness of brute forcing attacks.

[CommSec introduced password best practices](#) once Australia's Herald Sun approached the company, following two dismissed calls from the programmer:

"He said the online accounts used only a basic numeric password, rather than the secure and more common combination of alphabet and numeric characters. John said he was amazed the nation's biggest online trader was so vulnerable to cyber attacks and had called CommSec to notify them. After he made two attempts to explain the dire situation, the Sydney-based company dismissed his calls. John then contacted the Herald Sun in an attempt to have the issue addressed and online security upgraded."

The newly introduced password best practices come a month after another [security design flaw](#) was exposed at the online broker - [CommSec's use of non-SSL frames pages](#) potentially resulting in successful [man-in-the-middle attacks](#) . Sadly, the company is also not alone. Last year's published paper "*Analyzing Web sites for user-visible security design flaws* " stated that [75% of online banking sites are vulnerable to trivial security design flaws](#) similar to the ones exposed at CommSec.

And while the password best practices concern remain realistic even though brute forcing attempts would get easily detected, it's

worth emphasizing on the fact that even a SSL enabled, strong passwords empowered Ebanking session can be hijacked, once a [banker malware](#) like for instance, Zeus, Limbo or Adrenalin infects the host.

Online brand-jacking increasing | ZDNet

With the evolving sophistication of online scammers' understanding of social engineering and trust building online, the techniques they use to build authenticity into their scam propositions have started directly influencing a targeted brand's reputation online in the most negative way possible - the loss of a customer's trust into the brand's capabilities to defend itself against impersonation attacks.

[MarkMonitor's recently released Brandjacking Index 2008](#) indicates that brand-jacking is increasing, with online scammers actively abusing a brand's reputation in order to build more legitimacy into their campaigns, by taking advantage of the brand's trusted reputation. Some of the highlights in the report :

- On average, almost half a million instances of brand abuse were measured each week including 402,882 accounts of cybersquatting, the registration of domain names containing a brand, slogan or trademark to which the registrant has no right. Instances of cybersquatting rose 40 percent in the first quarter of 2008

- Media brands continue to be the most targeted by brandjackers with over 40,000 instances of abuse in Q1 2008. Abuse against automotive brands increased by 99 percent since Q1 2007 to 25,792

- Pay-per-click abuse continued to remain low in Q1 and is down 42 percent for the year. This form of brandjacking has experienced almost zero growth since Q2 2007. Vigilance by brandholders, regulatory changes by ICANN and policy changes by major search engines have driven the declines

- While brand abusers can be located anywhere in the world, their top countries for Web site hosting remained consistent. The U.S. is home to 66 percent of Web sites that host brand abuse. Germany hosts 7 percent, followed by the United Kingdom at 6 percent. Canada hosts 4 percent

As you can see cybersquatting to visually social engineer the visitor into thinking the site's legitimate, false association with

industry leading brands into the consumer protection business, as well as the phishing, represent the largest proportion of brandjacking techniques used. However, these are not mutually exclusive, and in reality often intersect with one another to provide a scammer with a multi-layered brandjacking capabilities. Let's discuss the most prevalent brandjacking tactics in details.

- Cybersquatting

The rise of cybersquatting can be explained with the overall availability of automatic domain registration software, which in a combination with automated approach to verify the availability of the domain and purchase it without the brand owner proactively monitoring for such abuse, is what's driving this increase. Some of the cybersquatted domains are in fact so creative, that would successfully spoof a brand's web application structure in the domain name, an example of which you can see in two [cybersquatted domain portfolios impersonating PayPal and Ebay](#) . In March, 2008, I assessed a domains portfolio registered by a single company known for its misleading business practices, that managed to brandjack security software brands such as [Pandasecurity, McAfee next to Adobe's Acrobat Reader](#) , with trustworthy looking domain names. Upon notification of the affected parties, the company expanded its portfolio, this time [cybersquatting Symantec's Norton Antivirus](#). All of these examples indicate a certain degree of centralization, namely, known companies and individuals continue cybersquatting some of the world's most popular brands, whose domains usually remain online for longer than they should be due to the brand's lack of proactive response to this tactic.

- False Association

You would purchase an item from a site that's been recommended by half the industry's leading anti-hacker monitoring services, and has all those "false feeling of safety and privacy" banners aiming to increase the trust of the potential buyer? The only difference between a rogue software site and the original one for instance, is that you would be able to click on any of these banners on the legitimate site and receive a response, whereas, there are no external links to click on at the bogus sites. This is where false

association comes into play, and it's something I've been monitoring for a while now. Basically, each and [every rogue security software](#) is quoting comments from leading industry benchmarks on how well it performs, and how many stars it's been awarded by a known service that tests and reviews software. And due to the overall availability of [web site templates for rogue security software](#) , on their way to scam as many people as possible, scammers often forget the take the time and effort to modify the template, ending up in amusing situations where the images promote a fake software while the text is promoting the old software included in the template. Knowing Dalai Lama doesn't mean Dalai Lama knows you, however, from a psychological perspective this is a very successful tactic that scammers would continue using.

- Phishing

Phishing is prone to increase given the direct scamming approach it utilizes in order to reach everyone, everywhere, in a combination with ongoing development of [do-it-yourself phishing kits](#) that I've assessed in a previous post. But the statistics released from the majority can be greatly engineered in respect to the changing tactics phishers take advantage of, such as hosting the phishing pages on breached sites courtesy of [the access provided by web site defacers](#) , and SQL [injecting them on vulnerable sites](#) , with the most recent case where the [U.K's Crime Reduction Portal](#) was hosting a phishing page.

Here are some of highlights on phishing discussed in the report :

- The number of organizations phished in Q1 remained steady over Q4 2007 at 408, representing an 8 percent rise for the year. The number of new organizations targeted by phishers decreased to 102 in Q1 2008
- 14 organizations account for 90 percent of all phishing URLs. Eight of these organizations are based in the U.S., and six are in the United Kingdom. 11 are financial institutions
- Phishing attacks against auction brands comprise 60 percent of all phish attacks in Q1 2008

- Phishing attacks against retail/service brands declined by 85 percent this quarter returning to Q1 2007 levels. This trend is evidence of the seasonal rise in phishing attacks against retail brands during the pre-holiday season

- 34 percent of phishing sites were hosted in the U.S. in Q1 2008 compared to 21 percent in Q4 2007

- Phishing URLs continued to decline in Q1 2008, evidence of continued influence from the Rock Phish Gang

A company wanting to protect its customers should either build an in-house capacity to monitor any brandjacking attempts, or outsource the process to vendors who have already build the capabilities to monitor, detect and respond to such attacks before a customer gets tricked. As for the customers, sometimes the bargain deal may be worst deal you've ever made if fall victim into a scammer targeting bargain hunters with propositions they simply cannot resist - but should.

Nuclear Pack exploit kit introduces anti-honeyclient crawling feature | ZDNet

For years, the security community has been developing efficient ways to evaluate the maliciousness of as many web sites as possible, by crawling them for malicious content in an automated fashion. Thanks to the rise of botnets as an exploitation platform, [today's cybercriminals](#) are largely relying on [compromised legitimate infrastructure](#) as a delivery vehicle for their malicious content, compared to using purely malicious sites as an infection/propagation vector.

Naturally, cybercriminals keep track of the latest anti-malware security research, and constantly adapt to the latest innovations by [introducing new features](#) within the most widely used [web malware exploitation kits](#).

[According to security researchers from ESET](#), while profiling yet another malware and exploits serving malicious campaign, they have stumbled upon a new feature introduced in the Nuclear Pack web malware exploitation kit.

More details:

We have tracked some interesting activity through the injected code block with iFrame redirection: Javascript code is used to capture mouse activity with the onmousemove event and only after that does malicious activity continue with the redirection. This activity enabled us to identify a simple method being used to bypass crawlers used by AV companies and others. These are the first steps towards the criminal's proactive detection of real user activity for tracking detections and bypassing malware collecting by whitehat crawlers.

The new feature is just the tip of the iceberg. Here are some of the most common evasive techniques used by cybercriminals to prevent vendors and security researchers from analyzing their campaigns:

The use of session-based cookies
The use of HTTP referrers to ensure the exploitation chain is

complete

The use of banned IPs of known security vendor netblocks

The use of OS fingerprinting/browser fingerprinting techniques

The serving of malicious content only once for a given IP address

Managed iFrame and JavaScript crypting/obfuscating services, dynamically introducing scripts with low-detection rates

For the time being, the [most widely used web malware exploitation kit](#) remains the [Black Hole exploit kit](#). Only time will tell whether its author will introduce the anti-crawling feature in the exploit kit, but given the fact that they introduce newly released exploits in a timely manner, it may already be on the "to-do" list of the cybercriminal behind the kit.

Norwegian BitTorrent tracker under DDoS attack | ZDNet

Norway's largest [BitTorrent tracker Norbits](#) (norbits.net) with approximately 10,000 users, is currently under [a DDoS attack launched from a group known as MORRADI](#), which is also speculating that it has managed to compromise the tracker and is threatening to release personal details of its users including IPs, until the tracker is closed :

"In [an NFO file obtained by IT-Avisen](#), a group called MORRADI takes responsibility for the attack on Norbits. "Once again we show our power! Once again we show your foolishness! This is not the first time we have done it, and it won't be the last," they write (translated).

"Enough is enough, you are becoming a real nuisance, and you are also a bunch of idiots that try to hide, so it's high time we punish you! P2P is not something we want, when will you understand that? Do we have to take it as far as publishing your user database online?"

This is [the second time the tracker has been under a DDoS attack](#) for the past two years, and no matter how futile the ambitions of the attackers are in respect to targeting the tracker due to the fact that it's promoting the use of P2P, the success of Norbits seems to have already pissed off the local warez scene.

Further investigation indicates a conflict of interest on the Norwegian warez scene, with old school FTP warez groups

clearly not in favor of emerging technologies like P2P directly undermining their outdated (pirated) content distribution models. The attack is very similar to an apparently still active campaign courtesy of old school warez traders, named "[Destroying The P2P's, One Step at a Time](#)", whose objective is to expose the owners of BitTorrent trackers, compromise their security and leak personally identifiable information of its users -- if such exists at the first place -- in order to damage their reputations.

Just when you through that the major threat a BitTorrent tracker faces is the threat from the entertainment industry and the local intellectual property enforcing organizations, [fractions of the "warez scene"](#) are waging a war against P2P. Will they also start targeting the mainstream torrent trackers?

North Korea ships malware-infected games to South Korean users, uses them to launch DDoS attacks | ZDNet

According to an [independent report](#) published in Korea's JoongAng Daily, Seoul's Metropolitan Police Agency has intercepted a cyber attack plot orchestrated by [North Korea's Reconnaissance General Bureau](#), which successfully shipped malware-infected games to South Korean users which were later on used to launch a DDoS attack against the web site of Incheon Airport.

More details:

According to the police, the South Korean man, identified by the surname Jo, traveled to Shenyang, northeastern China, starting in September 2009 and met agents of an alleged North Korean trading company. He allegedly asked them to develop game software to be used in the South.

Jo purchased dozens of computer game software for tens of millions of won, which was a third the cost of the same kind of software in the South. The games were infected with malignant viruses, of which Jo knew, an official at the police agency said.

Jo sold the games to South Korean operators of online games. When people played the games, the viruses used their computers as zombies, through which the cyberattack was launched.

This is the second attempt by North Korea in recent months to engage in electronic warfare with South Korea, following the [use of GPS jammers causing difficulties in air and marine traffic controls](#).

What's particularly interesting about North Korea's infection vector in this campaign, is that it's not a novel approach to spread malware. Instead, it relies on a chain of trust, from the unknown origin of the produced games, to the sellers claims that they are malware-free, and ultimately targets bargain hunters. In the past, [software piracy](#).

[has proven to be a key driving force](#) behind the growth of malware campaigns internationally.

Distribution of malware-infected games greatly reminds me of a case which happened in Eastern Europe in the 90s where a malware coder participating in a popular IT magazine's coding contest, on purposely backdoored his game, which ended being shipped to thousands of subscribers on a magazine-branded CD. Although a good example of a flawed QA (Quality Assurance) on behalf of the magazine, South Korean authorities claim that the person who purchased the games actually knew that they were infected with malware, hence the lower price for purchasing them.

Just how big of a cyber threat is North Korea? It's an emerging market player, having actively invested in the concept over the years, that's for sure.

In my recent [conversation with cyber warfare expert Jeffrey Carr](#), he pointed out that he doubts Russia or China will knowingly supply the irrational North Korea with cyber warfare 'know how'. However, Russia or China's chain of command doesn't need to know that [this outsourcing](#) will ever take place, as North Korea could easily [outsource to sophisticated cybercriminals](#) doing it for the money, not for the fame.

Who do you think currently poses a bigger cyber threat to the United States - [Russia](#), [China](#), [Iran](#) or [North Korea](#)?

TalkBack.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

No security software, no E-banking fraud claims for you | ZDNet

Rational, but unrealistic in today's threatscape. [According to the Times](#) :

"Customers using their credit or debit cards online have been advised that high street banks are likely to

become increasingly reluctant to help victims of internet fraud as new rules added to the Banking Code signal less willingness to cover losses. The updated code, which covers the banks' treatment of customers, came into effect last month and states that victims of online fraud must have up-to-date antivirus and antispyware software installed, plus a personal firewall, to claim redress from their banks. If you fail to have the correct protection in place, the banks are increasingly likely to refuse any claim for a refund."

The E-banking users are advised to have firewalls, antivirus software and protection from spam and phishing emails, to visit the sites of their software vendors and look for updates, and check for security certificates at the E-banking pages. There's also a realistic case study basically describing the real-life situation that having a perimeter defense in place is only decreasing the risk, not eliminating it entirely the way it's getting marketed :

"Andrew Omoshebi, a design engineer from North London, had £1,500 of fraudulent transactions on his credit card recently. The 43-year-old, left, uses his credit card only for online purchases and has all the necessary antivirus, antispyware and firewall protection installed on his computer. Even so, he was alarmed to discover three consecutive transactions on his statement that were not his."

Surprisingly, Apacs, the UK payments authority isn't mentioning anything about [blocking vulnerable browsers](#) from participating in any form of transaction with them, perhaps among the most strategic moves courtesy of PayPal compared to the marketable, but totally bypassed in real-life situations [PayPal's Security Key](#) . Why having

an antivirus software and a firewall doesn't mean anything from a malicious attacker's perspective?

Cross-site scripting [vulnerabilities within banking sites](#) are nothing new, in fact, in the past there were initiatives tracking down such vulnerabilities and how long it took for the bank to fix them. [Barclays is an example with XSS vulnerabilities](#) unfixed for over a year despite notification. Why aren't they taking XSS seriously at the first place? Because the people responsible for their anti-fraud activities aren't aware of the potential to abuse the vulnerabilities and use the bank site as a redirector to malicious software, or a phishing page with a decent SSL certificate in place. [Phishers are indeed using XSS vulnerabilities](#) to scam a bank's customers, thanks to the bank's vulnerable web applications, here's [the most recent incident](#) A lot of spam and phishing emails make it through antispam and phishing filters, what a lot of customers aren't getting educated about is that [spam and phishing emails can sometimes become a blended threat](#) , and include drive-by downloads that would automatically install on a vulnerable machine upon visiting the pages. From a psychological perspective, a lot of users are naturally interested in calculating the ROI of their antispam/antiphishing product, and therefore may visit a scam pages just to see whether or not their solution will pick it up, a practice which leaves a lot of opportunities for the bad guys to take advantage of

In 2007 and early 2008, client-side vulnerabilities continue dominating the infection vector of choice, not only because of their integration within popular web malware exploitation kits, but because diversifying the exploits set used increases the chances for a successful penetration from a malicious attacker's perspective. Whereas the article is suggesting that users update their Microsoft software, it ignores the fact that the majority of software used on an average PC is far more diverse than IE and Microsoft Office only, consequently, the rest of the software used would remain unpatched Keylogging for E-banking data is so dead, I cannot believe that customers are still educated about the trojan horse that would record their random number valid for a single session only. In reality, there's [a specific segment of malware](#) defined as [bankers malware](#) , whose features, sophistication, and targeted nature in the sense of having

researched the web applications of all the major banks, are going way beyond simple keylogging

Perimeter defense is marketable, yet irrelevant from an attacker's perspective, an attacker that would [ensure his malware releases make it through the most popular firewalls](#) before releasing the malware for instance. Would you be so naive to do E-banking from the local Internet cafe? The way you wouldn't do this, you also wouldn't want your PC to turn into an Internet cafe one, where everyone does pretty much whatever they want to, then leave. Emphasize on protecting against client-side vulnerabilities by using handy tools such as [Secunia's Personal Software Inspector](#) , and sacrifice some of your E-banking mobility by not doing it whenever you see a PC with Internet connection on it - else you're crying to claim fraudulent activities on your bank account.

New worm exploiting MS08-067 flaw spotted in the wild | ZDNet

Microsoft's [Security Response Center](#) and McAfee are warning on [increased network scanning activity](#) during the last couple of days courtesy of the very latest W32/Conficker.worm exploiting the already [patched MS08-067 vulnerability](#). What's particularly interesting in the latest wave of copycat worms is that [W32/Conficker.worm](#) is patching the infected host in order to ensure that competing malicious parties wouldn't be able to get in using it. How nice of them.

"This malware mostly spreads within corporations but also was reported by several hundred home users. It opens a random port between port 1024 and 10000 and acts like a web server. It propagates to random computers on the network by exploiting MS08-067. Once the remote computer is exploited, that computer will download a copy of the worm via HTTP using the random port opened by the worm. The worm often uses a .JPG extension when copied over and then it is saved to the local system folder as a random named dll. It is also interesting to note that the worm patches the vulnerable API in memory so the machine will not be vulnerable anymore. It is not that the malware authors care so much about the computer as they want to make sure that other malware will not take it over too."

The public release of the proof of concept code in September, prompted an immediate reaction by international underground communities releasing several different modifications of the exploit, with the Chinese to be first to release a [do-it-yourself tool](#) allowing subnet scanning and automatic exposure to malware hosted on a third-party server. At first, the [tool was released with commercial intentions](#) with its authors charging \$37.80, however, just like the majority of proprietary web malware exploitation kits, several days later the tool leaked to the general public. From a strategic perspective, whereas such DIY tools indeed empower low-profile

cybercriminals, the real danger comes from scanning modules introduced within larger botnets.

New variants of premium rate SMS trojan 'RuFraud' detected in the wild | ZDNet

Researchers from AegisLab, have [intercepted several new variants of the infamous RuFraud](#) premium rate SMS trojan.

How the infection takes place:

In order to earn money from the premium-rate SMS, the trojan will fake itself as a famous app, like Angry Birds; or downloader/installer of well-known softwares, it looks like 'real thing'. Some of these kinds of apps appear on the third-party download sites, and some will repackage itself, post to the official Android Marketplace, and try to lure innocent people to install it.

The malicious attackers have bundled the premium rate SMS trojan into a fake copy of the popular app Angry Birds. Upon execution, the trojan seems permissions to sent SMS messages. Once the user confirms that the application is free to do so, the trojan will start sending premium rate SMS messages to multiple numbers outlined in [AegisLab's post](#).

New Symbian-based mobile worm circulating in the wild | ZDNet

F-Secure and [Fortinet are investigating](#) a newly discovered [mobile malware](#) identified as [SymbOS/Yxes.A!worm](#) or "Sexy View". The malware is affecting S60 3rd Edition series devices, and has a valid certificate signed by Symbian tricking the mobile device user into thinking it's a legitimate application. In terms of propagation, "Sexy View" propagates by collecting all the phone numbers from the infected device, and then SMS-es itself to all of them including a link to a web site hosting a copy of it.

SymbOS/Yxes.A!worm is the second mobile malware detected in the wild for 2009, followed by last month's discovery of [Trojan-SMS.Python.Flocker](#) by Kaspersky Labs. A trend, a fad, or opportunists experimenting for mobile malware's prime time in 2009?

Using spam and phishing as analogies, both, spammers and phishers require huge databases of harvested email address in order to hit them directly. What used to be old-fashioned directory attacks where they were attempting to guess user names and associate them with email boxes, is today's [greatly matured underground market segment](#) offering millions of segmented (on per country, city, industry, email provided basis) emails which cybecriminals easily integrate within their campaign management kits.

What's particularly interesting about SymbOS/Yxes.A!worm is that it appears that the worm's main objective is to harvest information from the infected devices such as phone numbers, IMEI, IMSI as well as the phone type. This data harvesting approach is pretty similar to that of email harvesting tools, and in the long term the harvested data will be monetized and resold to phone scammers whose activities are already driving the success of such site as [WhoCallsme?](#) and [800notes](#) .

Moreover, [Guillaume Lovet](#) , a senior manager of Fortinet's Threat Research Team is also speculating on the potential for a mobile botnet due to the ways in which Yxes.A!worm spreads: "As far as

our analysis goes, the worm currently does not take commands from the remote servers it contacts. However, since the copies hosted on the malicious servers are controlled by the cyber criminals, they may update them whenever they want, thereby effectively mutating the worm, adding or removing functionality. We're really at the edge of a mobile botnet here. "

With carriers, manufacturers, and service providers clearly aware of the emerging mobile malware threat, thankfully, they seem to be thinking in the right direction - according to [McAfee's 2009's Mobile Security Report](#) , when asked "*Who Should Bear the Cost of Securing Mobile Devices?* " 44% of the mobile device manufacturers forwarded the responsibility to themselves instead of their clients.

In times when your mobile number and physical location for a successful scam targeting is prone to become a valuable good in the underground economy, your vigilance remains a cost-effective solution.

New study details the dynamics of successful phishing | ZDNet

Can you teach an old employee new phishing protection tricks?

In a recently presented [study by the Intrepidus Group](#), the company behind the [PhishMe.com](#) spear phishing awareness service allowing companies to ethically attempt to phish their employees on their way to build security awareness, [presents some interesting key findings](#) based on 32 phishing scenarios tested against a total of 69,000 employees around the world. Here they are:

23% of people worldwide are vulnerable to targeted/spear phishing attacks

Phishing attacks that use an authoritative tone are 40% more successful than those that attempt to lure people through reward-giving

Men and women are both equally susceptible to phishing

On an average 60% of corporate employees that were found susceptible to targeted spear phishing responded to the phishing emails within three hours of receiving them

People are less cautious when clicking on active links in emails than when they are requested for sensitive data

Metrics are invaluable, but in this case the obsession with metrics can result in more insecurities since it excludes the possibility of blended threats. For instance, last year I was closely monitoring a similar [blended Skype phishing campaign](#), where the cybercriminals (lkbMan) were attempting to optimize the click-through rate of their campaign by [serving client-side exploits to the visitors](#), "just in case" if they find the site suspicious and do not enter any accounting data. For the time being the exploit is served instantly upon visiting the phishing site, however, the possibility for serving it only if the user hasn't entered anything and is leaving the site is always there.

Go through related phishing trends and tactics: [Research: 76% of phishing sites hosted on compromised servers](#); [Microsoft study debunks phishing profitability](#); [Phishers increasingly scamming other](#)

[phishers](#) ; [DIY phishing kits introducing new features](#) ; [Phishers apply quality assurance, start validating credit card numbers](#) ; [Lack of phishing attacks data sharing puts \\$300M at stake annually](#).

Considering one of the key points from Intrepidus Group's study, namely that "*People are less cautious when clicking on active links in emails than when they are requested for sensitive data* ", a phishing email should be treated as spam, namely (in a perfect world) it shouldn't be even allowed to reach the employee's mailbox. Otherwise, it appears that the trade-off for coming up with quality metrics on the current degree of security awareness in regard to phishing, is the potential exposure of the tested population against potential blended threats.

With managed localization services in the sense of dedicated translators of messages to be used in spam, phishing, and malware campaigns already a fact, the cybercrime ecosystem will soon be talking in a native language, and with the increasingly automated phishing tools whose features were once available to a more sophisticated crowd of cybecriminals, now available for free - the future of phishing looks promising.

The only threat that can outpace its growth [is the threat posed by the much more efficient and sophisticated financial data targeting tactic of using crimeware](#) targeting each and every E-banking site simultaneously upon successful infection.

New study claims that Chrome is the most secure browser | ZDNet

Which is the most secure browser around?

According to a [newly released study by Accuvant](#), that's Google's Chrome.

The Google-commissioned research emphasizes on several key points that would make up a secure browser, namely the integration of sandboxing, plug-in security, JIT hardening, ASLR, DEP, GS and URL blacklisting.

Key summary point:

The URL blacklisting services offered by all three browsers will stop fewer attacks than will go undetected. Both Google Chrome and Microsoft Internet Explorer implement state-of-the-art anti-exploitation technologies, but Mozilla Firefox lags behind without JIT hardening. While both Google Chrome and Microsoft Internet Explorer implement the same set of anti-exploitation technologies, Google Chrome's plug-in security and sandboxing architectures are implemented in a more thorough and comprehensive manner. Therefore, we believe Google Chrome is the browser that is most secured against attack.

Related posts:

[Internet Explorer 9 outperforms competing browsers in malware blocking test Study: IE8's SmartScreen leads in malware protection IE8 outperforms competing browsers in malware protection — again](#)

Moreover, according to the report Mozilla's Firefox has the highest vulnerability count compared to Google's Chrome and Microsoft's Internet Explorer. Firefox leads with 449 patched vulnerabilities, followed by Chrome with 321 and Internet Explorer with 168.

Would you switch browsers over the results from a comparative review such as this one commissioned by Google? Do you believe

that Chrome is indeed the most secure browser around, or are there other factors to consider as well?

Talkback.

New SpyEye plugin takes control of crimeware victims' webcam and microphone | ZDNet

Security researchers from Kaspersky have [profiled a new SpyEye plugin](#) known as **flashcamcontrol.dll**.

What does it do? Basically, it modifies an infected host's Flash permissions, allowing cybercriminals the opportunity to control and webcam and the microphone of the infected victims.

More details:

If an infected user visits the site of a specified bank and the browser processing the page requests a flash-document via a link from the first column, the webfakes.dll plugin (which runs in a browser context) detects that request and replaces it with an address from the second column – an address controlled by the intruders. As a result, the browser will load a malicious document from the intruder's server (statistiktop.com) instead of a flash document from the bank site.

It turned out that both flash documents merely create a window with a picture from the webcam. One of them sends a video stream to the intruder's server.

It appears that someone is experimenting, with long-term ambitions on their mind. [Face recognition for online banking as a concept](#) has been around for years, however, financial institutions globally have failed to implement the solution on a large scale. Personally, I believe that facial recognition as a value-added protection mechanism is a futile attempt to prevent a successful crimeware attack on the infected host.

Taking into consideration the fact that on the majority of occasions users don't know that they're infected with crimeware, a visual representation of the fact that a particular end user is indeed in front of the computer wouldn't change this. And now cybercriminals have

developed an efficient way to undermine the facial recognition process with ease.

This latest development once again proves that cybercriminals are steps ahead of the security industry, and will continue to innovate in an attempt to increase their fraudulently obtained revenues.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

New report details the prices within the cybercrime market | ZDNet

What's the price of a stolen credit card number? How much does it cost to buy actual bank credentials and transform them into physical credit cards? Does it really matter from whom you're buying all the stolen data, and what really drives the underground's black market for stolen goods? Let's find out.

A newly released report by PandaSecurity entitled "[The Cyber-Crime Black Market: Uncovered](#)", details in depth the dynamic market interactions multiple market participants have with each other, and attributes the successful growth model to the rise of undetected trojan horses and [crimeware](#) used to steal financial data from infected users.

Highlights from the study:

The most common positions within a cybercrime enterprise:

Programmers, Programmers, Tech experts, Hackers, Fraudsters, Hosted systems providers, Cashiers, Money mules, Tellers, Organization Leaders.

The 8 stages purchasing process:

The product, The contact, Try & Buy, Online testing, Minimum orders and bulk discounts, Specialized online stores, Methods of payment, Customer services and support

From customer support, to discounts for bulk orders of credit card numbers, the cybercrime ecosystem still continues relying on basic economic principles, whether they realize and admit it at all. Take for instance risk-forwarding.

Risk-forwarding within the cybercrime ecosystem has to do with not only bulk sale of unverified and stolen financial data to unverified and low profile resellers, but most importantly, through [the use of money mules](#). The process requires that average Internet users fall victims into quick cash earning schemes, where a bogus company

manages to trick them into signing an agreement where they accept to receive and forward fraudulently obtained funds.

No study can give a definite answer even on the average price for a particular underground good or service, given how vibrant the cybercrime ecosystem is. This can be best described using price volatility thinking in the context of having multiple vendors selling the same item. Whereas for the experienced seller the item is now a commodity commanding a lower and more static price, new market entrants looking for ways to undercut the experienced sellers will offer a discount, in fact, bonuses in the form of access to alternative services in case the purchase ever takes place.

See also:

[Microsoft study debunks phishing profitability Microsoft study debunks profitability of the underground economy Study finds the average price for renting a botnet The current state of the crimeware threat - Q&A](#)

What do you think? Do you believe that just because there are so many cybercriminals interested in committing cybercrime, they deny themselves the ability to better monetize infected hosts in terms of the internal competition? Is crimeware responsible for more leakage of financial data, compared to massive data breaches?

Talkback.

New ransomware variants spotted in the wild

| ZDNet

Security researchers from [TrendMicro](#), [F-Secure](#) and [Dr. Web](#) have intercepted two new ransomware variants currently circulating in the wild.

TrendMicro intercepted a new ransomware variant that compared to previous releases is infecting the Master Boot Record (MBR), thus, preventing the operating system from loading. Upon execution, the infected PC restarts and displays the ransom message requesting a payment in order for them to receive the unlock code.

Both F-Secure and Dr.Web have intercepted an identical ransomware variant. Upon execution it encrypts all files, by adding a .EnCiPhErEd file extension. End users are given the option to have 5 attempts to try and enter the unlock code, in between the malware deletes itself and leaves the files encrypted.

The ransomware displays the following message to infected users:

Attention! All your files are encrypted! You are using unlicensed programmes! To restore your files and access them, send code Ukrash or Paysafecard nominal value of EUR 50 to the email **koeserg@gmail.com** . You have 5 attempts to enter the code. If you exceed this of all data irretrievably spoiled. Be careful when you enter teh code!

Moreover, the vendors are emphasizing on the fact that the encryption in the ransomware variants (**SHA1: b8f60c64c70f03c263bf9e9261aa157a73864aaf**) is not as strong as the encryption used in previous versions of the infamous GPCode.

See related posts:

[Localized ransomware variants impersonate law enforcement agencies](#) [Microsoft themed ransomware variant spotted in the wild](#) [Copyright violation alert ransomware in the wild](#) [New ransomware variant uses false child porn accusations](#) [Mac OS X SMS](#)

ransomware - hype or real threat? Who's behind the GPcode ransomware?

Ransomware attacks are becoming increasingly prevalent across multiple countries, thanks to the added localization and better market segmentation of the prospective victims. Cybercriminals taking into consideration quality assurance as a process, and constantly looking for new ways to socially engineer end and corporate users into infecting themselves with ransomware variants.

End users are advised to avoid interacting with suspicious links found in spam emails, and to ensure that they're running the latest version of their third-party software, and browser plugins.

New ransomware variant uses false child porn accusations | ZDNet

Researchers from BitDefender have detected a new [ransomware variant currently spreading in the wild](#).

Once Trojan.Agent.ARVF locks down the infected PC, it displays a message saying that the PC is locked due to the fact that child pornography was found on the user's system and the fine of 500 rubles must be paid within 12 hours. The Task Manager, Windows Explorer and User Init Logon Application are either killed or overwritten by the trojan in an attempt to prevent users from killing it.

The scammers says the user must pay within 12 hours or the "child-porn" case will be forwarded to the local police and all data stored on the personal computer will be blocked or deleted, the operating system uninstalled and the BIOS erased.

In reality, the data will still be there and the BIOS will not be affected after the 12-hour deadline passes. But the PC will remain locked. **Paying the ransom will not unlock it. In-depth analysis of the malware revealed that there is no way to unlock the PC, so the promise of a code is false.**

The malware is currently spreading over links distributed over social networks. Users are advised to be extra vigilant when dealing with suspicious links.

New ransomware locks PCs, demands premium SMS for removal | ZDNet

UPDATE : Another [variant has been detected](#) .

Following the recently uncovered [hybrid scareware with elements of ransomware](#) , and last year's [GPcode ransomware](#) attacks, cybercriminals have once again demonstrated their interest in the concept of ransomware.

PandaLabs is reporting on a [newly discovered ransomware variant](#) which locks the affected user's PC, and demands a premium SMS in order to deactivate it.

[Trj/SMSlock.A](#) doesn't have any self-propagation functions and appears to be coming under the form of a typical fake codec that has been affecting users for over a week now. The message (in Russian) demands that the affected user sends an SMS with the pseudo-unique number to the given number in order to receive deactivation code. From a monetization perspective, the approach is pretty similar to the recent [Trojan-SMS.Python.Flocker mobile malware](#) which was transferring account credit, and mimicking the original functionality of the [RedBrowser mobile malware](#) which was automatically sending SMS messages to premium-rate numbers in 2006.

Just how dangerous is SMSlock.A? Compared to GPcode, it's the work of less technically sophisticated people, making it fairly easy to bypass. Dr.Web has even released [a generator for deactivation codes](#) so that affected users don't have to pay.

Ransomware is not a fad, that's for sure. In fact, [Trend Micro's Annual Threat Report: Cybercriminals are Working Faster than Ever](#) stated that ransomware attacks are prone to increase in a targeted fashion during Q2 of 2009. And whereas the current variants do not have self-propagation functions, their primary propagation vector remains the hundreds of currently active blackhat search engine optimization campaigns serving the ubiquitous fake codecs ([Cybercriminals syndicating Google Trends keywords to serve](#)

malware ; Massive comment spam attack on Digg.com leads to
malware).

New ransomware impersonates the U.S Department of Justice | ZDNet

Security researchers from Trusteer have [intercepted a ransomware variant](#) being pushed using the [Citadel crimeware platform](#).

The ransomware is pushed using drive-by malware attacks. Upon execution the following activities take place:

Once installed on the victim's computer, the ransomware locks-up the targeted machine and displays a warning message notifying the user that they have violated United States Federal Law. The web inject screen (below) claims the IP address belonging to the infected machine was identified by the Computer Crime & Intellectual Property Section as having visited websites that contain child pornography and other illegal content. In order to unlock their computer, the victim is instructed to pay a \$100 fine to the US Department of Justice using prepaid money card services. The payment service options presented to the victim are based on the geographic location of their IP address. For example, users with US IP addresses must pay using MoneyPak or Paysafecard.

What's particularly interesting about this campaign, is that it's a decent example of campaign optimization performed on behalf of the cybercriminals behind it, adding multiple monetization vectors in it. Not only will they earn revenue out of the ransomware variant, they will also be able to successfully hijack online banking transactions thanks to the Citadel crimeware that will also remain active on the system.

Ransomware is becoming increasingly prevalent these days, with multiple [new variants being detected on a periodic basis](#). This micro-payments driven business model is largely driven by the fact that source code for ransomware is publicly obtainable from selected vendors within the cybercrime ecosystem.

In the long term, cybercriminals will continue emphasizing on basic QA (quality assurance) processes such as localization of the

templates to the native languages of prospective victims. We're definitely going to see more brands, law enforcement agencies and departments impersonated in a systematic manner.

New mobile malware silently transfers account credit | ZDNet

Kaspersky Lab today [warned users of five newly found variants](#) of the [Trojan-SMS.Python.Flocker](#) mobile malware, targeting an [Indonesian mobile provider's service](#) allowing users to [transfer money or minutes to each other's](#) accounts. SMS Python Flocker is a known mobile malware family, whose previous versions used to automatically send SMS message from the infected mobile device to premium-rate numbers operated by the malware authors.

Once infected with the latest variant, the malware would transfer credit from the infected device by silently SMS-ing the provider's credit transfer service with the desired amount of credit.

Such mobile credit transfer services are used internationally, however, compared to simple cash/account credit transfers, in the long term mobile malware authors would continue looking for ways to steal hard cash. Since the first releases of the [RedBrowser](#) in 2006, which was silently sending SMS messages ([screenshots](#)) to premium-rate numbers, mobile malware authors have been looking for ways to monetize the infected devices. What has changed since then is the [growth of mobile payments](#) /m-payments and mobile wallets, whose popularity is proportionally empowering potential mobile malware authors with all the [purchasing power an infected device has](#) .

For the time being, among the main reasons why we still haven't witnessed an epidemic of mobile malware, is sadly because cybercriminals are making enough profit even without exploiting the fact that there are more people with mobile devices, than people with personal computers around the world.

New malware attack circulating on Facebook

| ZDNet

Researchers from GData have intercepted [a currently circulating Facebook malware attack](#), that spreads via chat messages.

Messages used for spreading

bist du das?? aaaaaahahahahaahahaha

“hey is this your ex?? lol [LINK]

„omg you look so cute [LINK]”

Once the user clicks on the shortened URL, he's exposed to a executable file that looks like an image file. Upon clicking on the executable a "Picture cannot be displayed" error message appears. In between the malware is stored in the Windows %TEMP% folder and executed.

Users are advised to be extra vigilant when dealing with links found on Facebook.

New Mac OS X trojan spotted in the wild | ZDNet

Security researchers from Intego, [have intercepted several new variants](#) of the [Flashback Mac OS X trojan](#).

According to the company, the new variants of the Flashback trojan use three different infection vectors in an attempt to trick end users into installing the malware.

More details on the infection vectors:

This new variant of the Flashback Trojan horse uses three methods to infect Macs. The malware first tries to install itself using one of two Java vulnerabilities. If this is successful, users will be infected with no intervention. If these vulnerabilities are not available – if the Macs have Java up to date – then it attempts a third method of installation, trying to fool users through a social engineering trick. The applet displays a self-signed certificate, claiming to be issued by Apple. Most users won't understand what this means, and click on Continue to allow the installation to continue.

Once the end user gets tricked into installing the malware, the Flashback trojan will patch web browsers and network applications in order to search for user names and passwords. Targeted web sites include, Google, Yahoo! CNN, numerous banking web sites, PayPal and many others. What's particularly interesting about the Flashback trojan is the fact that it has an auto-update feature periodically phoning back to several web sites in order to check for updates.

Intego is advising users running OS X 10.6, to update Java immediately.

New Mac OS X trojan poses as malicious PDF file | ZDNet

Security researchers from [Sophos](#) and [F-Secure](#) have spotted a currently circulating Mac OS X trojan.

[Trojan-Dropper:OSX/Revir.A](#) disguises as a malicious PDF file for spreading purposes. When users attempt to open the Chinese-language PDF file, it installs additional backdoor dubbed Imuler.A, which would give malicious hackers remote access to your Apple Mac computer:

"The malware then proceeds to install a backdoor, [Backdoor:OSX/Imuler.A](#), in the background. As of this writing, the C&C of the malware is just a bare Apache installation and is not capable of communicating with the backdoor yet. The domain was registered on March 21, 2011 and was last updated on May 21, 2011.

Since this malware sample was received from VirusTotal, we cannot exactly be sure about the method it uses to spread. The most probable way is sending via e-mail attachment. The author could be just testing the water to see if the sample is detected by different AV vendors."

Users are advised to avoid interacting with suspicious files, or [follow the mitigation advice offered here](#).

New MAC OS X scareware delivered through blackhat SEO | ZDNet

Researchers from Intego have intercepted [a new scareware sample targeting the MAC OS X](#).

Named the MACDefender, the scareware sample shows a bogus interface, insisting that the end user is infected, and that their OS is in an insecure state. The researchers emphasize on the social engineering elements of the scareware, including the fact that although the site shows a fake Windows screen, the scareware itself is a well designed Mac application with no spelling or grammar mistakes in its description.

The scareware will periodically open pornographic content on the affected Mac, in order to trick the users into thinking they're infected with malware. The scareware is sold for \$59,95, part of a scareware affiliate network targeting Mac OS X users in particular.

Users are advised to exercise extra caution when dealing with suspicious downloads, especially ones delivered through blackhat search engine optimization techniques.

See also:

[Researchers spot new Mac OS X malware](#) [Malware Watch: Free Mac OS X screensavers bundled with spyware](#) [Mac OS X SMS ransomware - hype or real threat?](#)

New Mac OS X malware with DDoS functionality spotted in the wild | ZDNet

[Security researchers](#) from [multiple](#) companies, have spotted a [new Mac OS X malware](#). Dubbed 'Tsunami', the malware's primary goal is to act as platform for executing distributed denial of service (DDoS) attacks.

What's particularly interesting about this backdoor, is the fact that malware coders have ported the malware bot from Linux to Mac OS X in an attempt to enter the Mac OS X market segment.

See also:

[Will Code Malware for Financial Incentives Coding Spyware and Malware for Hire](#)

More on the malware:

In addition to enabling DDoS attacks, the backdoor can enable a remote user to download files, such as additional malware or updates to the Tsunami code. The malware can also execute shell commands, giving it the ability to essentially take control of the affected machine. In terms of functionality, the Mac variant of the backdoor is similar to its older Linux brother, with only the IRC server, channel and password changed and the greatest difference being that it's a 64-bit Mach-O binary instead of an ELF binary.

The malware is currently detected as [OSX/Tsunami-A](#).

Related posts:

[New Mac OS X malware disables Apple's malware protection](#)
[Snow Leopard's malware protection only scans for two Trojans](#)
[Malware Watch: Free Mac OS X screensavers bundled with spyware](#)
[New MAC OS X scareware delivered through blackhat SEO](#)
[New Mac OS X trojan poses as malicious PDF file](#)
[Researchers spot new Mac OS X malware](#)
[Mac OS X malware posing as fake video codec discovered](#)
[New Mac OS X malware variant spotted](#)
[New Mac OS X email worm discovered](#)
[New Mac](#)

OS X DNS changer spreads through social engineering Mac OS X SMS ransomware - hype or real threat?

New Mac OS X malware variant spotted | ZDNet

Intego is reporting on a [newly discovered variant of a Mac OS X malware](#) first detected in 2004.

According to the company, the source code of the **OSX/HellRTS.D** is already being distributed across multiple forums, which could potentially allow malicious attackers to create new variants of it.

More details on the malware:

It sets up its own server and configures a server port and password

It duplicates itself, using the names of different applications, adding the new version to a user's login items, to ensure that it starts up at login. (These different names can make it hard to detect, not only in login items, but also in Activity Monitor.)

It can send e-mail with its own mail server, contact a remote server, and provide direct access to an infected Mac

It can also perform a number of operations such as providing remote screen-sharing access, shutting down or restarting a Mac, accessing an infected Mac's clipboard, and much more

According to the brief security memo, OSX/HellRTS.D *"is being distributed on a number of forums shows that it will be accessible to a large number of malicious users who may attempt to use it to attack Macs."*

A similar leak of source code took place in November, 2009, when [the source code for ikee iPhone worm became publicly available](#). The leak, however, didn't result in any new worm modifications back then.

Go through related posts: [Mac OS X SMS ransomware - hype or real threat?](#) ; [New Mac OS X email worm discovered \(May, 2009\)](#) ; [Mac OS X malware posing as fake video codec discovered \(June, 2009\)](#) ; [New Mac OS X DNS changer spreads through social engineering \(August, 2009\)](#) ; [iHacked: jailbroken iPhones compromised, \\$5 ransom demanded](#)

The company has rated the malware as low risk due to the fact that they are unaware of any infected Macs so far.

However, this rating shouldn't apply to you overall situational awareness ([See: How To Disable "Open Safe Files After Downloading" Feature In Safari](#)) on the fact that Mac OS X malware is no longer an urban legend, but a fully realistic event with Apple Inc. publicly admitting that "[***no system can be 100 percent immune from every threat***](#)".

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/> and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back these settings

CLOSE

Researchers demo wireless keyboard sniffer for Microsoft 27Mhz keyboards | ZDNet

Researchers from Remote-Exploit.org, the home of the BackTrack pen-testing Linux distribution, have recently released an open source [wireless keyboard sniffer Keykeriki](#) , capable of sniffing and decoding keystrokes of Microsoft 27Mhz based keyboards through [on-the-fly deciphering of XOR based encryption](#) .

Their [wartyping](#) -- decoding signals from wireless keyboards -- proof of concept is based on a [research paper](#) published by the group [one and a half years](#) ago:

"Now 1.5 years after releasing our whitepaper "27Mhz Wireless Keyboard Analysis Report" about wireless keyboard insecurities, we are proud to present the universal wireless keyboard sniffer: Keykeriki. This opensource hardware and software project enables every person to verify the security level of their own keyboard transmissions, and/or demonstrate the sniffing attacks (for educational purpose only). The hardware itself is designed to be small and versatile, it can be extended to currently undetected/unknown keyboard traffic, and/or hardware extensions, for example, a repeating module or amplifier."

According to their slides, it took them approximately 20 to 50 keystrokes in order to successfully recover the encryption key, which shouldn't come as a surprise taking into consideration the use of XOR encryption.

Moreover, the researchers aren't aware of any patching possibility to the affected 27Mhz keyboards, and point out that while [Logitech's "Secure Connect"](#) solution is in fact adding an additional layer of encryption, they intend to include decryption capability in future releases of [Keykeriki](#) , next to inspection of [2.4Ghz wireless devices](#) and keystroke injection on the affected keyboards.

Time to get yourself [a wired keyboard](#) ? Not necessarily, since [additional research](#) also proves that wired keyboards are also [susceptible to sniffing attacks](#) . The potential security implications

and potential for abuse, are pretty evident. However, it's worth pointing out that [with or without Keykeriki](#) , economies of scale centered mass keylogging and session hijacking for fraudulent purposes, would continue happening through the usual channels - botnets and crimeware.

Researcher reports a CSRF vulnerability in Facebook's App Center, earns \$5,000 | ZDNet

A security researcher going by the name AMol NAik, has [earned \\$5,000 bug bounty from Facebook Inc.](#) thanks to a CSRF vulnerability he reported to the Security Team of the world's most popular social networking site.

In order for a malicious attacker to add applications to a Facebook user's Applications list, he would have to trick him into visiting a specially crafted Web site.

More details on the PoC (proof of concept) code:

There are many new parameters added in this new feature. Parameter 'fb_dtsg' is like token and 'perm' are the permissions required by the apps. Parameters 'redirect_url','app_id' are app specific values. Remaining parameters seems static except 'new_perms' & 'orig_perms'. I started to play with these two dynamic params and after few attempts, I knew that these params no longer needed to add an app. Anti-CSRF tokens like 'fb_dtsg' supposed to get validated at server-side. I was shocked to see that in this new feature, somehow developer missed this point and it was possible to add app without 'fb_dtsg'. Bang!!

It took Facebook Inc. a day to fix the reported vulnerability.

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Researcher releases details on 6 SCADA vulnerabilities | ZDNet

Italian security researcher [Luigi Auriemma](#) has released details and proof of concept code for 6 vulnerabilities affecting popular SCADA systems.

The same researcher released [details on 34 SCADA vulnerabilities](#) in March, 2011.

The vulnerabilities range from denial of service attacks, to information disclosure, to complete remote code execution.

The affected products are:

[Beckhoff TwinCAT 'TCATSysSrv.exe' Network Packet Denial of Service Vulnerability](#) [Rockwell RSLogix Overflow Vulnerability](#) [Measuresoft ScadaPro Multiple Vulnerabilities](#) [Cogent DataHub Multiple Vulnerabilities](#) [AzeoTech DAQFacstory Stack Overflow](#) [Progea Movicon Multiple Vulnerabilities](#)

[Image courtesy of Woodward](#)

Researcher discovers Nokia S40 security vulnerabilities, demands 20,000 euros to release details | ZDNet

Will disclose Nokia s40 security vulnerabilities for money? Part of Security Exploration's research program, Adam

Gowdiak, a well known researcher with a decent history of uncovered security issues, [recently made an announcement regarding two security vulnerabilities](#) affecting the implementation of mobile Java used by Sun and Nokia in their products, as well as 14 other security issues affecting different [Nokia Series 40 devices](#), accompanied by 14000 lines of proof of concept code, all presented in a 178 pages research report. Where's the catch? He's asking for 20,000 euros per company for access to the paper and proof of concept code. Here's [an excerpt from his paper](#) entitled "J2ME Security Vulnerabilities 2008" :

"The initial motive for this work was to verify security of proprietary Nokia devices and its Series 40 Platform in particular. For many years, no major threat had been uncovered for this family of Nokia devices. All of that regardless of increasing devices complexity and their very closed nature. Unfortunately, in a security research world, closed source/platform and complexity never go along with security. Thus, the motive for the research.

This paper presents the results of the research conducted from Feb 2008 till Jul 2008 in the area of security of Nokia Series 40 Platform devices and Java 2 Micro Edition (J2ME). It also contains information pertaining to security vulnerabilities discovered during the research process as well as detailed discussion of universal and reliable exploitation techniques for the aforementioned family of Nokia devices."

Will vendors purchase the research, ignore it entirely, or try to reverse engineer his claims based on the already provided details in order not to pay?

While I'm fairly certain that they'll try to reverse engineer his claims in order not to entice other researchers into holding

their proof of concept code and start demanding financial incentives for the research they've done, since the vendors themselves didn't commission it at the first place, at least Gowdiak isn't threatening to release it in the wild unless the vendor pays under a deadline.

This very same situation happened last year, when Vulnerability Discovery and Analysis (VDA) Labs demanded \$5000 for a security vulnerability that they found in LinkedIn's toolbar, an offer that would have increased to \$10,000 unless LinkedIn didn't pay the price based on the deadline they set. [Here's a sample of the letter](#) :

"We've discovered an attack against the LinkedIn toolbar. If you are interested in the bug, we would like to give first right of refusal to purchase it. We'd also like to perform a more complete security audit of your products. We can help make the LinkedIn products more secure," DeMott stated in e-mail sent to LinkedIn on July 10, as viewed by CNET News.com.

The e-mail continues: "If you wouldn't like to buy it then we are happy to resell or release as a full disclosure to help prevent security issues arising on end users servers. We strongly believe in keeping users safe. We are unique in that we give vendors a first chance at the bugs we discover rather than selling to a third-party or releasing publicly. Please find the VDA Labs Value add document attached. If you'd like to buy the bug we will provide working attack code, so that you can verify the bug, before you send the check."

Being a hostage of someone else's research isn't a very comfortable situation, especially when millions of mobile device users' security could be at stake. But with mobile device vendors allocating bigger budgets for marketing than R&D in security, and not even raising awareness on basic threats thereby contributing to insecure habits that would become the cornerstone for efficient exploitation of mobile devices in the very near future, perhaps this is a the wake up call they need to take seriously this time. Case in point - [trivial security vulnerabilities in NFC mobile phones](#) that could have been taken care of if usability was balanced with security,

remain unpatched, some of them not even recognized as vulnerabilities yet.

The bottom line of this insecure by design mentality is an end user that's paying more attention to the quality of the camera of the device, and taking security as granted. However, once the trivial vulnerabilities start taking place in the moment when the user is actively using mobile banking, he'd be the first to blame the vendor for lack of security, forgetting that he accepted and got used to using an insecure device at the first place. So don't take security for granted.

Researcher demos SMS-based smartphone botnet | ZDNet

A security researcher has demonstrated an Android based, SMS-driven smartphone botnet. Presented at this year's [ShmooCon conference](#) , the proof-of-concept shows multiple phones accepting commands from a central location, with knowledge of the commands interface.

"A botnet control scenario is presented in which smartphone bots receive instructions through sms that are processed by a proxy between the GSM modem and the application layer, making the botnet messages transparent to the user. An Android version of the bot will be shown in action, and proof of concept code will be released for multiple platforms. "

Upon sending a simple SMS message to the already infected smartphones, the response in terms of the actions executed can be tailored to the needs of a malicious attacker looking to create a mobile phone based botnet for literally any kind of malicious purpose. (Here's a [video of the demonstration](#)) .

Last week, researchers from Indiana University and the City University of Hong Kong released another [Android based proof of concept malware](#) , this time attempting to "hear" credit card numbers. [The Soundminer](#) , a context-aware piece of malware, is the very latest indication that the academic community wants to stay [a step ahead of cybercriminals themselves](#) .

Related posts:

[Researchers use smudge attack, identify Android passcodes 68 percent of the time Man-in-the-middle attacks demoed on 4 smartphones](#)

What's the future of mobile malware and smartphone botnets? Sadly, the future looks bright. From social engineering driven malware infections on Android devices, to [flawed from a security perspective, efficiency-driven models](#) , malicious attackers remain

perfectly positioned to capitalize on these exploitation vectors, unless the average and enterprise users become aware of them.

Researcher: 50 percent of Mac OS X users still running outdated Java versions | ZDNet

According to [a tweet posted by Aleks Gostev](#), Chief Security Expert, Global Research and Analysis Team at Kaspersky Lab, 50% of the visitors to their newly launched [Flashback information site](#), are still running outdated versions of Java, potentially exposing themselves to numerous exploitation attempts courtesy of malicious attackers.

The cybercriminals behind the Flashback Mac OS X malware are exploiting [CVE-2011-3544](#) and [CVE-2012-0507](#) vulnerabilities in Java, and that's just for starters.

[According to Zscaler](#), hundreds of thousands of enterprise users remain exposed to malicious attacks, due to the fact that they're running outdated versions of their third-party software.

Here's the summary of their findings affecting, both, Mac OS X users and Windows users:

- Adobe Acrobat - 62.54% of out-dated plugins
- Adobe Shockwave - 35.69% of out-dated plugins
- Microsoft Outlook - 7.26% of out-dated plugins
- Java - 5.88% of out-dated plugins
- Adobe Flash - 4.37% of out-dated plugins
- Microsoft SilverLight - 1.73% of out-dated plugins
- QuickTime - 1.71% of out-dated plugins
- Windows Media - 1.25% of out-dated plugins
- RealPlayer - 0.23% of out-dated plugins

A malicious attacker targeting the Mac OS X platform, [doesn't need to take advantage of zero day vulnerabilities](#), due to the fact that end users continue failing to patch their third-party applications and browser plugins. What's particularly interesting in the Flashback Mac OS X malware attack, is the fact that the cybercriminals behind it took advantage of the delayed patch for Java under Apple's OS. Taking into consideration the percentages of end users still using the Web with outdated third-party applications

and browser plugins, multiple Flashback related campaigns could be launched relying on this fact.

Apple users, with [a patch for the Java vulnerabilities currently available](#), there's no excuse to avoid patching as soon as possible.

Research: Spammers actively harvesting emails from Twitter in real-time | ZDNet

Security researchers from WebSense, have conducted an experiment, proving that [Twitter is still a heaven for spammers](#) looking to harvest freshly shared email addresses.

More details on the experiment:

We conducted research on how data that might be considered private is exposed via Twitter. The research focused on shared data, in particular email addresses, that can potentially be used against the one (or the organization) that shared it. During the research we monitored Twitter over a 24 hour period and found that users were publicly sharing email addresses connected with their inboxes, social media identities, and bank accounts. This leaves them open to advanced 'social spear phishing' attacks and spam campaigns.

Our research found that thousands of Email addresses are publicly shared daily via Twitter. More than 11,000 email addresses were shared worldwide.

This isn't the first time that a vendor is aiming to raise awareness on the fact, users sharing their emails publicly, can become targets of successfully crafted spear phishing campaigns.

I little [experiment I conducted back in 2009](#), also provided similar results. Basically, what I did was to measure the trending of words such as "email me at"; or "contact me at". The results? Thousands of freshly shared emails ready to be harvested by spammers in real-time.

[Twitter email harvesters](#) have been in the wild for years, it's time for Twitter's users to wake up and realize that the spammers are monitoring Twitter's global feed, and are [successfully harvesting their email addresses](#).

Research: Small DIY botnets prevalent in enterprise networks | ZDNet

Does the size of a botnet really matter? It's all a matter of perspective.

Contrary to the “common wisdom” that based on their size, [big botnets](#) are theoretically capable of infiltrating a huge percentage of enterprise networks, a recently presented study entitled “[My Bots Are Not Yours! A case study of 600+ real-world living botnets](#)” shows an entirely different picture.

According to Gunter Ollmann, VP of research at Damballa, based on their observation of 600 different botnets within global enterprises throughout a period of three months, [small DIY botnets aiming to stay beneath the radar accounted for 57% of all botnets](#), and hence, [successfully evaded detection in most of the cases](#) :

“The average size of the 600 botnets we examined hovered in the 101-500 range on a daily basis. Why do I use the term “on a daily basis”? Because the number of active members within each botnet tend to change daily – based upon factors such as whether the compromised hosts were turned on or part of the enterprise network (e.g. laptops), whether or not they had been remediated, and whether or not the remote botnet master was interactively controlling them.

While many people focus on the biggest botnets circulating around the Internet, it appears that the smaller botnets are not only more prevalent within real-life enterprise environments, but that they’re also doing different things. And, in most cases, those “different things” are more dangerous since they’re more specific to the enterprise environment they’re operating within.”

Conducting corporate espionage through botnets is not a new concept. In fact, the practice of relying on targeted attacks for automatic abuse of corporate networks has been a successful approach for several years.

For instance, in 2007, researchers from Support Intelligence launched an initiative called "[30 Days of Bots](#) " aiming to highlight Fortune 1000 businesses sending out spam through malware infected hosts within their networks. Their initiative provided interesting results, emphasizing on the modest number of infected hosts found within the following companies:

[3M](#) ; [Thomson Financial](#) ; [AIG](#) ; [Aflac, Inc](#) ; [BusinessWeek](#) ; [Toshiba America Business Solutions](#) ; [Conseco](#) ; [Bank of America Securities](#) ; [Clear Channel](#) ; [Borders Group](#) ; [Affiliated Computer Services](#) ; [Nationwide Insurance](#) ; [ATA Airlines](#) ; [Intel](#) ; and [IndymacBank](#)

What the researchers from Support Intelligence did, is something cybecriminals have been doing and offering as a service for a while - data mining, or from their perspective, the ability to data mine a big botnet and [rent access to hosts](#) residing on particular networks not for the purpose of spam sending, but for targeted corporate espionage.

And whereas these small botnets are favored for conducting cyber espionage, the size of the botnet truly matters to [efficient cybercrime platforms](#) generating billions of spam, phishing and malware like some of the newly emerging "market players".

According to the just released [MessageLabs Intelligence report for August](#) , the Grum and Bobax botnets have overtaken the leading position of [Cutwail/Pushdo](#) , currently responsible for 23.2% and 15.7% of all spam respectively, with an estimated botnet size for Grum at 560k to 840k followed by Bobax with 80k to 120k infected IPs.

Research: Many mobile password managers offer false feeling of security | ZDNet

In a [newly published research](#) by [Elcomsoft's researchers](#), the company argues that many of the mobile secure password managers aren't as secure by design, as originally thought of.

In a paper entitled "[Secure Password Managers](#)" and "[Military-Grade Encryption](#)" on Smartphones: Oh, Really?", they review 17 popular passwords management apps available for Apple iOS, and Blackberry platforms such as:

BlackBerry's Device Backup, Keeper® Password & Data Vault, Password Safe - iPassSafe free version, My Eyes Only™ - Secure Password Manager, Strip Lite - Password Manager, Safe - Password, iSecure Lite - Password Manager, Ultimate Password Manager Free, Secret Folder Lite, as well as the following paid applications, SafeWallet - Password Manager, SplashID Safe for iPhone, DataVault Password Manager, mSecure, LastPass for Premium Customers, 1Password Pro, BlackBerry Password Keeper, and the BlackBerry Wallet.

Their conclusions? The most commonly encountered flaw, is the fact that the master password and user passwords are stored unencrypted, leading to potential compromise of the device thanks to a physical security breach.

Moreover, the vendor argues that "*Many password management apps offered on the market do not provide adequate level of security. We strongly encourage users not to rely on their protections but rather use iOS or BlackBerry security features*".

Go through the report in order to find out more about the test results for each and every paid, and free mobile application.

Research: 80% of Web users running unpatched versions of Flash/Acrobat | ZDNet

According to a [research published by Trusteer](#) earlier this month, 79.5% of the 2.5 million users of their Rapport security service run a vulnerable version of Adobe Flash, with 83.5% also running a vulnerable version of Acrobat.

The company has also criticized Adobe by insisting that their update mechanism "*does not meet the requirements of a system that is used by 99% of users on the Internet and is highly targeted by criminals*", but is praising the update mechanism of Google's Chrome and Firefox, whose [silent updates close the window of opportunity](#) for malicious attackers to take advantage of.

Trusteer's research findings come a month after Secunia found out that [Adobe is shipping an insecure version of Reader from its official site](#), justifying the action with the built-in updater, which apparently is not used by the 2.5 million users mentioned in the research, followed by an advice given in the [SANS NewsBites newsletter, issue 61](#), that organizations should limit the use of Adobe products in order to minimize the attack surface.

Due to the high market penetration of Adobe's products, it's fairly logical to witness an increase of malicious exploitation of Adobe related vulnerabilities. However, there aren't any web malware exploitation kits in the wild that are exclusively relying on Adobe-specific vulnerabilities. Instead, the exploits-mix that is served upon successful browser recognition attempts to exploit the most common applications found on a particular PC in order to increase the probability of successful infection.

Data published by Secunia two months ago, indicates the same trend that cybercriminals have been aware of for a while now, namely, that [the average insecure program per PC rate is still high](#), with 3 insecure programs in the U.S on average, and 4 insecure programs per PC in Europe based on the company's data. The company [published similar findings two years](#), providing that an

unpatched vulnerability is just as handy as a zero day one from the perspective of the cybercriminal who's efficiently infecting hundreds of thousands of users by exploiting outdated/unpatched flaws.

Adobe's products aren't an exception, they're targeted in between the rest of the vulnerabilities included in the exploits-mix. Don't just make sure that you're running the latest version of Flash and Reader, make sure that you're [running the latest versions](#) of all the [applications on your PC](#) , before cybercriminals do the check for you.

Research: 80% of Carberp infected computers had antivirus software installed | ZDNet

Just how useful is antivirus software in general? According to a [recently published study by security researcher Jim Mc Kenney](#), based on his analysis 80% of Carberp infected computers had antivirus software installed, which was either disabled, or crippled by the Carberp malware leaving antivirus users with a 'false feeling of security'.

The forensic investigation included 603 computers located in Kansas, Missouri, Oklahoma and Nebraska. What he found was pretty interesting. The majority of users relying on Symantec's Norton 360 antivirus had their protection either crippled or completely disabled. The same happened to AVG, Microsoft's Security Essentials, McAfee, Avast, ESET, Sophos, Avira, Kaspersky and BitDefender users.

Are the findings of this study a trend or a fad? Sadly, the [cybercriminals' ability to bypass antivirus protection](#) is an emerging trend within the cybercrime ecosystem, rendering popular antivirus solutions completely useless.

This isn't the first study confirming that sophisticated crimeware releases completely bypass antivirus solutions, by either disabling them, or by ensuring that their malicious releases would remain undetected even if executed on a host running an antivirus solution.

In 2009, Trusteer published [an advisory that measured the in-the-wild effectiveness of antivirus solutions](#) against the most popular crimeware, the Zeus crimeware. Their advisory concluded that "*The effectiveness of an up to date anti virus against Zeus is thus not 100%, not 90%, not even 50% - it's just 23%.*" and indicated that 55% of users infected with the Zeus crimeware were running an up-to-date antivirus solution.

Prevention is always better than the cure. Ensure that you're always running and [up-to-date third-party software](#) and [browser plugins](#) as on the majority of occasions cybercriminals will [attempt to exploit](#) outdated and already [patched vulnerabilities](#), next to coming up with creative ways to socially engineer you to execute a malicious executable.

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Research: 76% of phishing sites hosted on compromised servers | ZDNet

In a [newly released paper](#) entitled "[Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing](#)" Tyler Moore and Richard Clayton provide empirical evidence according to which 75.8% of the phishing sites that they've analyzed (2486 sites) were hosted on compromised web servers to which the phishers obtained access through Google hacking techniques (search engine reconnaissance).

The research also indicates that not only are legitimate sites (unknowingly) providing hosting services to scammers, but also that 19% of the vulnerable sites that they've analyzed were recompromised within six months.

This efficient exploitation approach using "evil searches" is in fact so efficient, that the majority of [large scale SQL injection attacks](#) that took place in 2008 were performing [automatic search engine reconnaissance](#) and later on exploiting the affected sites.

The trend has proven itself with cases where for instance the web sites of [U.K's Crime Reduction Portal](#) , a [Police Academy in India](#) , [government servers across the world](#) and even [a Chinese bank](#) were all hosting phishing pages through the exploitation of their web servers.

Go through related phishing tactics and trends - [Microsoft study debunks phishing profitability](#) ; [Phishers increasingly scamming other phishers](#) ; [DIY phishing kits introducing new features](#) ; [Phishers apply quality assurance, start validating credit card numbers](#) ; [Lack of phishing attacks data sharing puts \\$300M at stake annually](#).

Search engine reconnaissance or "[Google hacking](#)" is a legitimate penetration testing practice that cybercriminals naturally take advantage of as well.

However, the long tail effect that they manage to successfully achieve through the automatic [syndication of the very latest web application vulnerabilities within their botnets](#) will continue resulting

in such disturbing reports claiming that [500,000 web sites were successfully SQL injected in 2008 alone](#) .

The bottom line - if you don't take care of your web application based vulnerabilities, someone else will. And yes, they will come back six months later to find out whether the web servers still remain vulnerable.

Image courtesy of [PhishTank's February Statistics](#) .

Research: 1.3 million malicious ads viewed daily | ZDNet

[New research released by Dasient](#) indicates that based on their sample, 1.3 million malicious ads are viewed per day, with 59 percent of them representing [drive-by downloads](#), followed by 41 percent of [fake security software](#) also known as scareware.

The attack vector, known as [malvertising](#), has been increasingly trending as a tactic of choice for numerous malicious attackers, due to the wide reach of the campaign once they manage to trick a legitimate publisher into accepting it.

More findings from their research:

The probability of a user getting infected from a malvertisement is twice as likely on a weekend and the average lifetime of a malvertisement is 7.3 days

97% of Fortune 500 web sites are at a high risk of getting infected with malware due to external partners (such as javascript widget providers, ad networks, and/or packaged software providers)

Fortune 500 web sites have such a high risk because 69% of them use external Javascript to render portions of their sites and 64% of them are running outdated web applications

The research's findings are also backed up by another recently released report by Google's Security Team, stating that [fake AV is accounting for 50 percent of all malware delivered via ads](#).

The increased probability of infection during the weekend can be attributed to a well known tactic used by the individual/gang behind the campaign. Once [the social engineering part takes place](#), in an attempt to evade detection, they would first feature a legitimate ad, wait for the weekend to come thinking that no one would react to the attack even if it was reported, and show the true face of the campaign.

Case in point is [NYTimes malvertising campaign](#) (Sept. 2009):

The creator of the malicious ads posed as Vonage, the Internet telephone company, and persuaded NYTimes.com to run ads that initially appeared as real ads for Vonage. At some point, possibly late Friday, the campaign switched to displaying the virus warnings. Because The Times thought the campaign came straight from Vonage, which has advertised on the site before, it allowed the advertiser to use an outside vendor that it had not vetted to actually deliver the ads, Ms. McNulty said. That allowed the switch to take place.

Why would a malicious attacker engage in malvertising attacks, compared to relying on hundreds of thousands of compromised sites?

Malvertising is not an exclusive practice used by [a team of cybercriminals](#) specializing it in. It's done [in between the rest of the malicious campaigns and activities](#) the gang/individual is involved into.

From a cybercriminal's perspective, a high trafficked web site would naturally mean greater click-through rates, or as we've seen in previous cases, actual pop-ups of the ubiquitous fake scanning progress screen. Moreover, when direct compromise of this host cannot take place, they would attempt to locate and abuse the weakest link in the trust chain, in this case the third-party advertising network having access to the site. The problem then multiplies due to the re-syndication of the ad inventory from a particular publisher to another.

Related posts: [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Scareware pops-up at FoxNews](#) ; [Gawker Media tricked into featuring malicious Suzuki ads](#) ; [MSN Norway serving Flash exploits through malvertising](#)

One of the main problems publishers face, is that in order to stay competitive in the marketplace, they emphasize more on the efficiency of acquiring new customers, compared to the security practices that would prevent such a attack from taking place, and clearly that also includes the use of [commercial anti-malvertising solutions](#) .

This efficiency vs security approach can be best seen in a [major malvertising campaign profiled in February, 2010](#), where the malicious attackers targeted as many efficiency-centered publishers as possible, successfully infiltrating known services, such as [DoubleClick](#) and [Yieldmanager](#).

In an attempt to trick the average end user who may get suspicious and realize that a scareware pop-up appeared through a malicious ad, the attackers included a "*visual social engineering*" element, by naming the subdomains using the trusted Google Analytics brand.

In terms of protection from an end user's perspective, Windows users browsing the Web in a [sandboxed environment](#), using [least privilege accounts](#), [NoScript for Firefox](#), and ensuring that they are [free of client-side exploitable flaws](#), will mitigate a huge percentage of the risk.

Have you been a victim of malvertising? When and where was the last time you were exposed to a bogus scareware "*You're infected*" pop up? Who should be held responsible, the publisher for accepting the ads and the lack of automatic malicious content scanning mechanisms, the site that featured it, or the end user for his lack of situational awareness on what malvertising and scareware is in general?

Talkback, and share your opinion.

Reports: SQL injection attacks and malware led to most data breaches | ZDNet

With millions of personal records and payment card information stolen on a regular basis, several recently released reports independently confirm some of the main sources of breaches. Not surprisingly, that's not zero day flaws, not even insiders, but good old fashioned [SQL injections](#) next to malware infections.

With companies investing more resources into ensuring their networks and employees are protected against the very latest threats, some are clearly overlooking the most basic threats, usually requiring simple or average attack sophistication on behalf of the cybercriminal.

Let's review the reports detailing the true impact of SQL injections and malware in the context of data breaches.

- UK Security Breach Investigations Report - An Analysis of Data Compromise Cases - 2010

Safe's recently released [Breach Report for 2010](#) , states that based on the analysis performed by their forensic investigations, 40% of all the attacks relied on SQL injections, with another 20%, a combination of SQL injection attacks and malware. Not only was the source of the attack external in 80% of the cases, but also, a weakness in a web interface was exploited in 86% of the cases, with the majority of affected companies operating in a shared hosting environment.

See how Chinese hackers and botnet masters launch massive SQL injection attacks using public search engines: [Massive SQL Injection Attacks - the Chinese Way](#) ; [SQL Injection Through Search Engines Reconnaissance](#) ; [Massive SQL Injections Through Search Engine's Reconnaissance - Part Two](#)

- Trustwave's Global Security Report 2010

[Trustwave's Global Security Report for 2010](#) , offers similar insights related the use of SQL injections (third position in the initial

attack entry list) for obtaining unauthorized access to payment card information. The report makes an interesting observation, stating that based on their analysis in 81% of the cases the compromised computers were managed by a third-party, compared to the 13% self-managing themselves.

Furthermore, the report details the most common types of malware that contributed to the loss of customer data, stating that in 54% of the cases the attackers harvested the data in transit.

What malware types were the attackers relying on? [Memory parsers \(67% of the cases\)](#), followed by malware using keylogging (18% of the cases) and network sniffing (9%) of the tactics, and 6% of the cases using credentialed malware, also known as ATM malware ([Diebold ATMs infected with credit card skimming malware](#)).

Related posts: [Scammers caught backdooring chip and PIN terminals](#) ; [Scammers introduce ATM skimmers with built-in SMS notification](#) ; [Microsoft study debunks profitability of the underground economy](#) ; [CardCops: Stolen credit card details getting cheaper](#)

With such basic attack techniques, it shouldn't be surprising that the data exfiltration methods used clearly speak for the insecure state of the companies in question, with Microsoft Windows Network Shares used in 28% of the cases, followed by Native Remote Access Application (27%) and File Transfer Protocol used in 17% of the cases. As far as encrypted channels are concerned, Trustwave's report states that they've only found a single case of an encrypted channel used to exfiltrate the data from the company's network.

- The Poneman Institute - Cost of a Data Breach

Despite that [the report emphasizes on](#) recommendations and [includes valuable metrics](#) to be considered in a cost-benefit analysis, it also states that based on their research, data breaches due to malware attacks doubled from 2008 to 2009, with the cost of a data breach due to a malicious attack higher than the cost of breaches caused by negligent insider or system glitches. Interestingly, it also states that notifying affected customers right away costs more than delaying the notification. That's of course from the perspective of the customer, not the affected customer whose financial data may have

already been abused for fraudulent purchases, depending on the data breach in question.

- Verizon's 2009 Anatomy of a Data Breach Report

Last but not least, is [Verizon's 2009 Anatomy of a Data Breach Report](#) , according to which malware and SQL injections were the main sources of the data breaches, as well as responsible for the majority of exposed records. Clearly, this average combination of attack tactics is surprisingly effective against companies who not just supposed to, but obliged by law to have properly secured their infrastructure.

How do cybercriminals know that these corporations are susceptible to such easily, and often exploitable in a point'n'click fashion flaws? Are they shooting into the dark, or do they rely on some kind of methodology which assumes that the low hanging fruit is an inseparable part of every thought to be secure network? Here are some of key issues to consider:

- The KISS (Keep It Simple Stupid) principle within the cybercrime ecosystem

A cybercriminal that doesn't have a clue about what he's doing -- government sponsored/tolerated cyber spies and cyber warfare units are an exception although the KISS principle still applies -- would spend months preparing, possibly investing huge amounts of money into buying a zero day vulnerability into a popular web browser in an attempt to use it in gaining access to the company's network. A pragmatic cybercriminal, would on the other hand be ["keeping it simple"](#) , and would logically assume that there's a right probability that the company overlooked the simplest threats, which he can easily exploit.

Go through related posts: [Research: Small DIY botnets prevalent in enterprise networks](#) ; [Research: 80% of Web users running unpatched versions of Flash/Acrobat](#) ; [Secunia: Average insecure program per PC rate remains high](#)

With such a realistic mentality, and due to the fact that the cost of executing these attacks is so small, intentionally or unintentionally he comes to the conclusion that the perceived level of security within an

organization, appears to be misleading. In this case, complexity is fought with simplicity, starting from the basic assumption that technologies are managed by people, and are therefore susceptible to human errors which once detected and exploited could undermine the much more complex security strategy in place.

The same mentality is applicable to a huge percentage of the "botnet success stories" over the past few years. Instead of assuming that the millions of prospective victims have patched their operating systems ([Does software piracy lead to higher malware infection rates?](#)), next to all the third-party software running on their hosts, and start look for ways to obtain the much desired zero day vulnerability, a cybercriminal would basically assume that the more client-side vulnerabilities are added to a particular web malware exploitation kit, the higher the probability for infection.

And sadly, he'd be right.

- The role of automated web application vulnerability scanning in the process of achieving a (false) feeling of security

A report "[Analyzing the Accuracy and Time Costs of WebApplication Security Scanners](#)" published earlier this month, indicated that Point and Shoot, as well as Trained scanning performed with the scanners, missed 49% of the vulnerabilities they were supposed to detect. The report also pointed out that the scanners that missed most of the vulnerabilities, also reported the highest number of false positive, the worst possible combination. Clearly, what's more dangerous than insecurity in general ([Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems](#)), is the false feeling of security.

Remember [China's much-speculated "unhackable OS" Kylin](#), which was perceived as a threat to the offensive cyber warfare capabilities of other nations, who've spent years building them on the basis of known operating systems? Just like any other operating system, it's weakness is in the balance -- or the lack of such -- of usability vs security, in this case it's the insecurely configured web applications that would allow the attackers to reach the level of usability offered to legitimate users.

Not by investing resources into looking for OS-specific flaws, but by exploiting the "[the upper layers of the OSI Model](#)". It's not just more cost effective, it's just that sometimes the attackers keep it simple.

Why do you think companies neglect the simplest threats, which are also the ones with the highest risk exposure factor due to their ease of exploitation? What do you think?

TalkBack.

Report: Zeus crimeware kit, malicious PDFs drive growth of cybercrime | ZDNet

Symantec's recently released "[Internet Security Threat Report trends for 2009](#)" report, takes a deep dive into the world of cybercrime, by discussing some of the key driving forces behind its growth.

From the affordable price of the [ubiquitous crimeware kit Zeus](#), to the tremendous [growth of malicious PDFs seen in 2009](#) based on the integration of Adobe flaws in popular malware kits, the report describes a cybercrime ecosystem whose entry barriers are becoming increasingly lower.

Key findings of the study:

In 2009, the United States had the most overall malicious activity, with 19 percent of the total; this is a decrease from 23 percent in 2008, when the United States also ranked first

The company observed 6,798,338 distinct bot-infected computers during this period; this is a 28 percent decrease from 2008

Symantec created 2,895,802 new malicious code signatures in 2009, a 71 percent increase over 2008

The top attacked vulnerability for 2009 was the Microsoft Windows "[SMB2' Smb2ValidateproviderCallback\(\)' remote Code Execution Vulnerability](#)".

Of all browsers Symantec analyzed in 2009, Safari had the longest window of (vulnerability) exposure with a 13-day average

Attack type "*PDF Suspicious File Download*" accounted for 49% of Web-based attacks for 2009. In comparison the use of malicious PDFs in 2008 was 11%.

Crimeware kits like Zeus make it easier for unskilled attackers to compromise computers and steal information

Although the report is attributing the growth of cybercrime to the right factors, there's one element of the cybercrime ecosystem that has more effect than the overall availability and affordable price of the Zeus kit - the [Cybercrime-as-a-Service \(CaaS\) market model](#).

Related services: [Spamming vendor launches managed spamming service](#) ; [76Service - Cybercrime as a Service Going Mainstream](#) ; [Zeus Crimeware as a Service Going Mainstream](#)

What's more dangerous? The ever-decreasing price of the ZeuS crimeware kit, or the trending availability of Cybercrime-as-a-service propositions? Just how significant as a threat is the Zeus crimeware kit?

Not surprisingly, the company is contributing the growth of ZeuS crimeware generated malware -- in 2009, Symantec observed nearly 90,000 unique variants of binary files created by the Zeus toolkit -- to the combination of its affordable price, and the increasing number of people performing online banking activities.

The company is not alone in observing the growth and success of the ZeuS crimeware kit.

September, 2009's "[Measuring the in-the-wild effectiveness of Antivirus against Zeus](#) " report by Trusteer, indicated that *"the effectiveness of an up to date anti virus against Zeus is thus not 100%, not 90%, not even 50% - it's just 23%."* meaning that cybercriminals have clearly started excelling into [the practice of bypassing signature-based malware scanners](#).

[APWG Phishing Activity Trends Report for Q3 of 2009](#) , also pointed out that based on the 22,754,847 scanned computers [15.89 percent were infected with banker malware](#). Moreover, Trusteer's latest data shows that one in every 3,000 computers from the 5.5m hosts they monitor in the US and UK, is [currently infected with ZeuS](#).

Combined with the new features in the latest version of ZeuS ([code protection with hardware-based licensing system](#)), the kit's authors are clearly interested in strengthening their position as market leader of crimeware activity online:

The new version of Zeus targets the growing population of Firefox users, in addition to Internet Explorer. Previous versions were incapable of exploiting Firefox to commit sophisticated online fraud against banks using strong layers of authentication. However, Zeus 1.4 supports HTML injection and transaction tampering for Firefox,

two techniques which are effectively used to bypass strong authentication and transaction signing solutions.

It's clear that cybercriminals operate in an environment so comfortable, that it allows them to achieve their fraudulent objectives much easily than they used to a few years ago.

The keyword for ensuring that you don't become one of the millions of people infected with Zeus or malware in general, is "situational awareness", next to the basic common sense tips for preventing a possible infection.

Report: third party programs rather than Microsoft programs responsible for most vulnerabilities | ZDNet

According to Secunia's recently released "[Yearly Vulnerability Research Report](#)", third party applications rather than Microsoft programs are responsible for the majority of vulnerabilities.

Moreover, the report further confirms a popular myth which I already debunked in my "[Seven myths about zero day vulnerabilities debunked](#)" post, namely that [patched vulnerabilities remain the the primary exploitation vector](#) that malicious attackers take advantage of.

More from the report:

For all Secunia Advisories affecting a typical end-point in 2011, 72% had a patch available within one day of the disclosure of the vulnerability, and 77% of the advisories had a patch available within 30 days of disclosure.

This data indicates that there is limited room for 0-day exploits. The 28% of the advisories that had no patch available on the day of disclosure indicates an upperbound of potential for 0-day exploit availability. Microsoft even reports that less than 1% of the attacks in the first half of 2011 were attributed to 0-day exploits. Therefore, the mere possibility of 0-day exploits, a force majeure, does not justify ignoring 72% of the cases where effective remediation is possible and at users' fingertips. Thus, organisations can hardly hide behind the threat of 0-days when a solution is available for 72% of vulnerabilities.

Averaged over a year, 2.7% of the Microsoft programs are found insecure compared to 6.5% of the third-party programs. Thus, on average, more than twice as many third-party programs are found unpatched than Microsoft programs.

What does this mean? It means that end and corporate users continue utilizing the potential of the Internet while using outdated

third-party applications and browser plugins. In the past, Secunia has released detailed statistics on the [average number of insecure applications per country](#), with Cuba and North America topping the chart.

End users are advised to ensure that they're using the [latest versions of their third-party software](#), and [browser plugins](#).

Related posts:

[37 percent of users browsing the Web with insecure Java versions](#)
[Kaspersky: 12 different vulnerabilities detected on every PC](#) [56 percent of enterprise users using vulnerable Adobe Reader plugins](#)

Report: Patched vulnerabilities remain prime exploitation vector | ZDNet

Which is the most popular tactic that cybercriminals use on their way to infect users with malicious code (malware) and [generate yet another botnet](#) ?

According to a [newly released report](#) by M86 Security, that's patched vulnerabilities. Why are cybercriminals turning to the exploitation of outdated flaws in the first place? Sadly, because it works taking into consideration the [average insecure 3rd party application/plugin on a sample PC](#) . Are cybercriminals being picky? Not at all, as thanks to web malware exploitation kits such as Eleonore, Phoenix, Unique Pack, Crime Pack or Fragus, they always exploit whatever is exploitable on a targeted host.

The top 10 most observed vulnerabilities served by web malware exploitation kits:

- Microsoft Internet Explorer RDS ActiveX
- Office Web Components Active Script Execution
- Microsoft Video Streaming (DirectShow) ActiveX Vulnerability
- Real Player IERPctl Remote Code Execution
- Adobe Acrobat and Adobe Reader CollectEmailInfo
- Adobe Reader GetIcon JavaScript Method Buffer Overflow
- Adobe Reader util.printf() JavaScript Func() Stack Overflow
- Microsoft Internet Explorer Deleted Object Event Handling
- Microsoft Access Snapshot Viewer ActiveX Control
- Adobe Reader media.newPlayer

Next to the above mentioned flaws, the report is also emphasizing the fact that, in the second half of 2010, Java-based attacks rose to higher levels than anticipated.

The trend is confirmed by a second [recently released report](#) . According to Cisco's data, the exploitation of patched Java flaws has outpaced exploitation through the use of malicious PDF files, at 6.5 percent on average for 4Q10. The increase of this exploitation

technique is once again contributed to the use of specific web malware exploitation kits.

See also:

[Seven myths about zero day vulnerabilities debunked](#) [Report: Apple had the most vulnerabilities throughout 2005-2010](#) [Report: Zeus crimeware kit, malicious PDFs drive growth of cybercrime](#) [Report: 64% of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts](#)

Users are advised to use [least privilege accounts](#) , [browse the web](#) in [isolated environment](#) , and ensure their [hosts are free](#) of [outdated 3rd party software](#) , [browser plugins](#) or OS-specific flaws.

Report: malware pushed by affiliate networks remains the primary growth factor of the cybercrime ecosystem | ZDNet

According to [FireEye's](#) recently released "[FireEye Advanced Threat Report 2H 2011](#)" report, malware pushed by affiliate networks -- also known as pay-per-install networks -- remains among the key growth factors of the cybercrime ecosystem.

Key summary points from the report:

The fastest growing malware categories in the second half of 2011 were PPI (pay per installs) and information stealers.

Of the thousands of malware families, the "Top 50" generated 80% of successful malware infections.

Over 95% of enterprise networks have a security gap despite \$20B spent annually on IT security.

Spear phishing attacks increase when enterprise security operations centers are lightly staffed or understaffed, particularly during holidays.

What's so special about pay-per-install malware? It's the fact that malicious attacker earns revenue every time a successful infection takes place, due to his participation in an affiliate program offering high payout rates for infected PCs.

More details:

In the second half of 2011, pay-per-install (PPI) downloaders, worms, backdoors, and information stealers represented the four most prevalent categories of malware. PPIs are malware programs that charge a fee to download or distribute other malware programs. These programs differ from normal downloaders/droppers in that a PPI malware author gets paid for every successful install of another malware program. Of the top four malware categories, information stealers and backdoors present the greatest threat to enterprises.

Next to the growth of pay-per-install malware applications, FireEye observed an increased in Zbot and Sality information steals. The

company attributed the growth of Zbot also known as the Zeus crimeware, to the leaked source code, allowing potential cybercriminals to easily modify and tailor the source code to their needs.

The company is also seeing an [increase in the use of the BlackHole web malware exploitation kit](#), thanks to the [constant updates issued by its authors](#), currently targeting a diverse mix of client-side vulnerabilities.

Consider going through FireEye's report [here](#).

Report: Malicious PDF files comprised 80 percent of all exploits for 2009 | ZDNet

[A newly released report](#) shows that based on more than a trillion Web requests processed in 2009, the use of malicious PDF files exploiting flaws in [Adobe Reader](#) / [Adobe Acrobat](#) not only outpaced the use of [Flash exploits](#) , but also, grew to 80% of all exploits the company encountered throughout the year.

Are the flaws in [Adobe's product line](#) becoming the cybercriminal's favorite exploitation tactic? Depends, since from another perspective malicious attackers don't have preferences, they exploit whatever is exploitable.

As seen in figures 8 and 9, malicious PDF files comprised 56% of exploits in 1Q09, growing to 80% of all exploits by 4Q09. Conversely, Flash exploits dropped from 40% in 1Q09 to 18% in 4Q09. This trend is likely indicative of attackers' preference for PDF exploit, probably due to a combination of increasing availability of vulnerabilities in Adobe Reader and Adobe Acrobat and the continued widespread use and acceptance of PDF files in both the workplace and consumer sectors.

Although [the report is establishing a logical connection](#) between the increasing availability of Adobe exploits based on the number of vulnerabilities reported in Adobe's products, it doesn't emphasize on an important fact.

From a cybercriminal's perspective, traffic optimization has evolved from exploit-specific wide-scale attacks, to today's cybercrime business model driven by web malware exploitation kits automatically enumerating potentially exploitable applications and browser plugins, and serving them the appropriate exploits. This malicious optimization of traffic has been an active strategy for several years, with the attackers realizing that the more exploits they introduce within their kits, the higher the probability of infection.

Chart courtesy of [Trusteer research](#) published in August, 2009

Therefore, the increasing use of malicious PDFs can also be interpreted as the direct result of the millions of users using outdated and exploitable Adobe products, with the only preference a malicious attacker could have in this case remaining the incentive based on the [99% penetration of Adobe Flash on Internet-enabled PCs](#) . But how is it possible that with such a high market share, ScanSafe's report shows that Adobe Acrobat/Reader exploits grew [while the use of Flash exploits declined?](#)

Naturally, there are malicious attackers with clear preferences, based on a number of factors. Some of the widespread client-side exploit serving campaigns launched in the wild over the past few months, act as a good example of how [cybercriminals actively monitor the metrics generated from their malicious campaigns](#) , and tailor their [exploitation tactics based on third-party application or browser plugins](#) that contributed to most of the successful infections.

Consider going through analysis of the malicious campaigns: [IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild](#) ; [Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild](#) ; [PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild](#) ; [Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits](#) ; [Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams](#) ; [Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware](#)

What these campaigns have in common, is the clear preference towards using Adobe Acrobat/Reader exploits only. Interestingly, the [cybercriminals maintaining them are also relying on the KISS principle \(Keep It Simple Stupid\)](#) , since the campaigns are not necessarily exploiting the very latest flaws in Adobe's product line.

Case in point is the exclusive use of [CVE-2007-5659](#) ; [CVE-2008-2992](#) ; [CVE-2008-0015](#) ; [CVE-2009-0927](#) ; and [CVE-2009-4324](#) , with their choice either based on the already gathered metrics, which not surprisingly include traffic logs based on the hundreds of thousands of visitors hitting their fraudulent online properties. In this case, why would they bother buying a zero day on the underground

market, when they already know that millions of end users are susceptible to exploits released two years ago? They won't.

Despite that the data speaks for itself, Adobe's products are among the countless number of applications and browser plugins that you're currently using. [Making sure that you're running the latest versions](#) , combined with the use of a browser allowing you to [take full control of your browsing experience with security in mind](#) , is highly recommended.

What do you think - are Adobe's products insecure in general, [is the company leaving the "window of opportunity" wide open for too long](#) , or are their products on the top of the exploitation list due to the fact that millions of users continue using old versions of the company's software?

TalkBack.

Report: malicious PDF files becoming the attack vector of choice | ZDNet

[According to a newly released report](#) by Symantec's MessageLabs, malicious PDF files outpace the distribution of related malicious attachments used in targeted attacks, and currently represent the attack vector of choice for malicious attackers compared to media, help files, HTMLs and executables.

The report also notes a slight increase in the distribution of executable files, a rather surprising trend given the fact that spam and email filters will definitely pick them up.

PDFs now account for a larger proportion of document file types used as attack vectors. However, it should be noted that office-based file formats are still a popular and effective choice used in some targeted attacks. In 2009, approximately 52.6% of targeted attacks used PDF exploits, compared with 65.0% in 2010, an increase of 12.4%. Despite a recent downturn in the last three months, if this trend were to continue at the same rate it has for the last year, the chart in figure 2 shows that by mid-2011, 76% of targeted malware could be used for PDF-based attacks.

PDF-based malware campaigns are here to stay, though:

"PDF-based targeted attacks are here to stay, and are predicted to worsen as malware authors continue to innovate in the delivery, construction and obfuscation of the techniques necessary for this type of malware ," said MessageLabs Intelligence Senior Analyst, **Paul Wood** .

Are cybercriminals picky? Not necessarily as it's entirely based on the campaign in question. In this case, they appear to be interested in bypassing spam and email filters by distributing a ubiquitous filetype that's often allow to pass through them in the first place.

Email attachments combined with social engineering tactics, are among the many attack vectors, cybercriminals take advantage of. Next to email attachments, the use of web malware exploitation kits is growing, with the majority of publicly obtainable data indicating

that they continue [relying on outdated and already patched vulnerabilities for successful exploitation](#) .

See also:

[Report: Patched vulnerabilities remain prime exploitation vector](#)
[Report: Zeus crimeware kit, malicious PDFs drive growth of cybercrime](#) [Report: AV users still get infected with malware](#) [Seven myths about zero day vulnerabilities debunked](#)

Report: Large US bank hit by 20 different crimeware families | ZDNet

For years, cybercriminals have been systematically undermining the effectiveness of antivirus software, successfully reaching a "malicious economies of scale" stage in their ambitions to steal money from affected parties across the globe.

One of the major shifts in their strategy over the past couple of years, is the professionalism applied to malicious campaigns targeting the weakest link in the entire trust chain - a bank's customers. Instead of trying to directly compromise the infrastructure of a specific financial institution and steal money from the inside, cybercriminals have been busy developing advanced and efficient ways to steal these very same money from a bank's customers.

In 2012, are cybercriminals still busy coming up with ways to directly compromise a financial institution's infrastructure? It appears so, at least according to [recently released Trusteer advisory](#), indicating that during their research they found over 20 different crimeware families on a single host within a large U.S bank during a period of 12 months.

Were these targeted attacks, or good old fashioned massive spamvertised campaigns? Based on the fact that the host was infected with such a wide variety of crimeware, it appears that the host has been compromised by multiple cybercriminals/gangs of cybercriminals, who managed to trick the user behind this host, over and over again, resulting in the messy situation.

Although enterprises get compromised on a daily basis, Trusteer's findings are more of a fad, then a trend. How come? Pretty simple, its easier to target a bank's customer, compared to attempting to somehow compromise the bank's infrastructure, and cybercriminals know that already, hence their malicious campaigns orbit around this fact and will continue to do so.

What do you think? Will cybercriminals attempt more sophisticated attacks against the infrastructure of financial institutions, compared

to targeting the weakest link in the trust process - the bank's customers?

TalkBack.

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Report: Google's reCAPTCHA flawed | ZDNet

UPDATED: According to a Google representative from the Google Global Communications & Public Affairs who contacted me - *"While the report is newly released, its substance is not current and seems to include some misunderstandings of the reCAPTCHA technology according to some of our engineers. Therefore, the so-called flaws described in the report, are not related to the reCAPTCHA that people use today."*

In a newly [released report](#), security researcher claims that Google's [reCAPTCHA](#), one of the most widely adopted free CAPTCHA services, contains weaknesses that would allow a 10,000 infected hosts botnet the ability to achieve 10 recognition successes every second, allowing it to register 864,000 new accounts per day.

In response, [a Google spokesman stated](#) that the report relies on data collected in early 2008, and doesn't take into consideration the effectiveness of the current technology used against machine solvers.

More from [the report](#) :

Running against 200 challenges, this method solved 10 correctly - a success rate of 5 percent. It further got one word correct in 25 other cases. If we presume that in half the cases the failed word would be the unknown word for reCaptcha, this gives us a total success rate of 17.5 percent. Also worth noting, ocrpus alone solved 0 of the 200 challenges. When ocrpus was provided with the challenge split into single word portions it was able to get 5 single words, a success rate of 1.25 percent.

For instance, with a 10,000 machine botnet (which would be considered relatively small these days), given broadband connections and multi-threaded attack code, even with only 10 threads per machine, a 0.01% success rate would yield 10 successes every second, which would provide the attacker with 864,000 new accounts per day if they were attacking a registration interface.

Here comes the [actual problem posed by the real threat](#) - on their way to emphasize on the "human factor" ([Google's CAPTCHA experiment and the human factor](#)) in the CAPTCHA recognition process in terms of usability, it becomes easier for the vendors in the CAPTCHA solving economy ([Inside India's CAPTCHA solving economy](#)) to efficiently solve them, this time with a 100% success rate. Therefore, Google's reCAPTCHA is just as flawed as any other CAPTCHA.

The underground economy has long adapted to the CAPTCHA recognition process, and the number of crowd-sourcing driven services offering access to APIs providing hundreds of thousands of recognized CAPTCHA for major Web 2.0 sites and social networks, is increasing. Naturally, it shouldn't come to as a surprise that the price for bulk orders of a million recognized CAPTCHAs is decreasing.

One such service that's promoting itself as a mainstream reCAPTCHA solver, is currently offering **1 million solved reCAPTCHAs for \$800** , with special prices for custom packages. On the other hand, the Koobface botnet, once a [customer of such commercial CAPTCHA recognition services](#) , is now achieving a 100% success rate by forcing the Koobface-infected users into recognizing them, who by doing so are unknowingly helping the botnet efficiently register thousands of accounts across multiple web properties. Clearly, the long-term emphasis appears to be on the 100% success rate offered by humans who knowingly or unknowingly solve CAPTCHAs for fraudulent purposes.

Is machine-learning CAPTCHA breaking an outdated approach used by spammers, in comparison to the emerging CAPTCHA solving services relying exclusively on humans, the very same humans that the CAPTCHA was originally meant to identify?

What do you think? Talkback.

Report: Conficker and AutoRun infections proliferating | ZDNet

According to [ESET's most recently released ThreatSense Report](#), two of the most prevalent threats for the year of 2011 remain AutoRun infections, followed by [Conficker infections](#).

ESET attributed the growth of AutoRun and Conficker infections to millions of Internet-connected pirated copies of Windows XP and Vista, not able to receive Microsoft's updates thanks to the Windows Genuine Advantage wall.

[Microsoft disabled AutoRun on Windows XP and Windows Vista](#) machines in February, 2011, leading to a [significant decline in AutoRun infections](#), at least according to Microsoft' sensor networks.

[Software piracy, indeed leads to a higher malware infection rates.](#)

What do you think?

Talkback.

Report: AV users still get infected with malware | ZDNet

According to [data released by EUROSTAT](#) , the European Union's statistics agency, one third of internet users in the EU caught a computer virus, despite the fact that 84% of internet users used IT security software (anti-virus, anti-spam or firewall) for protection.

In 2010 in the EU27, a large majority of individuals (84%) who used the internet in the last 12 months stated that they used an IT security software or tool to protect their private computer and data. Among the Member States, more than 90% of internet users in the Netherlands (96%), Luxembourg, Malta and Finland (all 91%) used IT security software, while it was less than two-thirds in Latvia (62%), Romania (64%) and Estonia (65%).

Countries with the most infected users:

- Bulgaria (58%)
- Malta (50%)
- Slovakia (47%)
- Hungary (46%)
- Italy (45%)
- Germany (22%)
- Finland (20%)
- Ireland (15%)
- Austria (14%)

In similar findings accompanying EUROSTAT's data, PandaLabs recently released data indicates that in January, [50 percent of computers worldwide were infected with some type of computer threat](#) , in this case, trojan horse, allowing malicious attackers access to a victim's host as well as to financial data.

50 percent of all computers scanned around the globe in January were infected with some kind of malware. As for the most damaging malware threat, Trojans caused the most incidents (59 percent of all cases), followed by traditional viruses (12 percent) and worms (9 percent). The list of most prevalent malware threats is topped by

generic Trojans, followed by downloaders, exploits and adware. It is worth mentioning the presence of Lineage, an old Trojan that continues to spread and infect systems.

[Does this mean that security software is ineffective at all?](#) Not necessarily, as it has to do with successful social engineering attacks, even expanding window of opportunity for malicious attackers to take advantage of, by the time their latest "release" gets the (automatic) attention of an antivirus company.

The bottom line? [Prevention](#) is [always](#) better [than](#) the [cure](#) .

Correction: The original headline "Report: 87% of AV users still got infected with malware" to this post was incorrect and has been changed.

Report: AutoRun malware infections continue topping the charts | ZDNet

Despite [Microsoft's response to the rise of AutoRun malware infections](#) in February, 2011, according to [ESET's recently released](#) telemetry data for 2012, [the infection vector](#) tops their chart for a second year in a row.

What seems to be the problem?

It's called [software piracy](#) , which has the capacity to lead to the successful compromise of a host, thanks to the outdated third-party software and operating system that it's running, as well as the often backdoored software cracks/key generators distributed to gullible users.

In 2009, the Business Software Alliance (BSA) [released a report](#) connecting the high malware infection rates of several countries, to the piracy rate corresponding to the same countries. In a blog post back then, [Symantec also speculated](#) that "The lack of patching due to piracy may be a contributory factor to high infection rates in those countries."

Does software piracy automatically translate into a successful malware infection on the host in question? It can greatly contribute to such an event, taking into consideration the fact that millions of Internet connected users within developing countries are currently online using pirated versions of Microsoft's Windows OS, preventing them from obtaining the latest security patches, including the one that's preventing the abuse of the AutoRun feature.

When speculating on the logical connection between software piracy and malware infection rates, it's worth emphasizing the fact that, on a large scale, cybercriminals tend to exploit browser/browser plugin specific flaws, compared to actually building an inventory of client-side exploits targeting popular third-party software, and OS specific flaws. At least that's what I've been observing over the past couple of years, an observation which naturally excludes targeted attacks/cyber espionage campaigns which can utilize these.

With this in mind, it shouldn't be surprising that AutoRun infections continue topping ESET's charts, years after Microsoft took care of the problem, and even [reported a decline in this type of infections](#) thanks to their response to the issue. It's basically [users running a pirated/outdated version of their Windows OS](#) .

What do you think? If not software piracy, what's still contributing to the existence of AutoRun infections, years after Microsoft (supposedly) fixed the problem?

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Report: Apple had the most vulnerabilities throughout 2005-2010 | ZDNet

Which vendor has the most reported security vulnerabilities?

According to [Secunia's recently released report](#), between 2005 and 2010 that's Apple Inc. followed by Oracle and Microsoft. Moreover, based on the company's data, ten vendors are responsible for 38% of the total number of vulnerabilities, and seven of the vendors on the top 10 list back in 2005, still occupy the top positions in 2010.

However, interpreting this data through the prism of the [current threat landscape](#), results in some pretty interesting findings. For instance, although Apple visibly tops the graph, excluding [social engineering driven malware attacks targeting Mac OS X users](#), there are no known widespread campaigns utilizing any of these vulnerabilities -- targeted attacks and cyber espionage attacks excluded.

Moreover, although Adobe is on the 5th position, in 2009 [malicious PDFs represented 80 percent of all exploits](#), followed by active [exploitation of Flash](#) taking into consideration the fact that millions of users continue browsing the Web using outdated versions of Adobe's products.

Related posts:

[Secunia: Average insecure program per PC rate remains high](#)
[Report: 48% of 22 million scanned computers infected with malware](#)
[Report: 64% of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts](#)
[Report: Malicious PDF files comprised 80 percent of all exploits for 2009](#)
[Research: 80% of Web users running unpatched versions of Flash/Adobe](#)

Even though Microsoft's Windows remains the top target due to its market share, which through the eyes of the cybercriminal means solid ROI (return on investment) given the modest investment, it's worth pointing out that [3rd party apps and plugins in particular](#), compared to Microsoft OS/Microsoft product specific vulnerabilities,

is what the cybercriminals continue using as their primary means of exploitation.

On a large scale, the shift from vendor/application specific, to "target them all" exploitation tactics, is pretty evident. Thanks to the growth of web malware exploitation kits, literally exploiting whatever is exploitable on a targeted host, through the diverse set of (outdated/already patched) exploits they come with, cybercriminals no longer shoot in the dark. They shoot at everything that hits they malicious, or compromised legitimate sites.

Being the vendor with the most reported security vulnerabilities, doesn't necessarily mean being the most insecure one, as it all comes down to "prevention is better than the cure" processes, defense in depth strategies, and patch management strategies. That's of course [if end uses and companies are aware, and are actually patching](#), something which is clearly not happening.

Does Apple's position on the top of graph mean its products are more insecure than those of Oracle and Microsoft? Does the vulnerability count for a particular company really matter, given the fact that the growth of cybercrime in 2010 is largely driven by outdated vulnerabilities -- meaning users just don't care? Is Microsoft feeling all the heat thanks to the millions of end users running outdated 3rd party applications and plugins on the top of its OSs?

What do you think? Talkback.

Report: 92% of critical Microsoft vulnerabilities mitigated by Least Privilege accounts | ZDNet

A recently [released report](#) by BeyondTrust entitled "[Reducing the Threat from Microsoft Vulnerabilities](#) " indicates that according to the company's analysis of all the security bulletins Microsoft published in 2008, 92% of the critical vulnerabilities could have been mitigated by the [principle of the least privilege](#) .

Despite the fact that Microsoft's products continue topping the "successfully exploited charts" in each and every web malware exploitation kit ([go through](#) sample [infection rates](#)), long gone are the days when Microsoft's products are targeted exclusively. Nowadays, in order to better optimize a malware campaign, [a web malware exploitation kit](#) is targeting a diverse set of client-side software/browser plugins.

Here are some of the key points from the report :

92% of Critical Microsoft vulnerabilities are mitigated by configuring users to operate without administrator rights

Of the total published Microsoft vulnerabilities, 69% are mitigated by removing administrator rights

By removing administrator rights companies will be better protected against exploitation of 94% of Microsoft Office, 89% of Internet Explorer, and 53% of Microsoft Windows vulnerabilities

87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights

Interestingly, starting from the basic fact that the client-side vulnerabilities exploited through the web exploitation kits have had their associated patches for months, sometimes years, end users appear to not only lack understanding of least privilege accounts, but also, still believe that patching their browser is where [the self-auditing process](#) both, starts and ends.

Moreover, the ongoing [Conficker/Downadup malware campaign](#) which has already passed the 10 million infected hosts milestone, is a very recent example of another phenomenon - the fact that millions of end users and possibly companies, are on purposely using pirated copies of Windows and are therefore using highly vulnerable, yet Internet connected, versions of it. The proof? [Symantec's geolocated graph of infected Conficker hosts speaks for itself](#) , as the countries having the [highest software piracy rate](#) , are in fact the ones most heavily hit by the malware.

However, least privilege accounts can always be used by both, legitimate users and software pirates altogether, which when combined with a decent situational awareness in the sense of knowing the current attack tactics, is prone to decrease their chance of getting successfully compromised.

Report: 64% of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts | ZDNet

According to a newly released report, [64% of all the reported Microsoft vulnerabilities for 2009](#) could have been mitigated by using the principle of the least privileged accounts.

By collecting data from Microsoft's Security Bulletins published throughout the year, and identifying the vulnerabilities who would have been mitigated by users whose accounts are configured to have fewer user rights on the system, BeyondTrust's quantitative report message is simple - get back to the basics.

Key summary points on the percentage of flaws mitigated:

90% of Critical Windows 7 operating system vulnerabilities are mitigated by having users log in as standard users

100% of Microsoft Office vulnerabilities reported in 2009

94% of Internet Explorer and 100% of IE 8 vulnerabilities reported in 2009

64% of all Microsoft vulnerabilities reported in 2009

87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights

The window of opportunity -- [21 days in the case of this out-of-band IE patch](#) -- often left wide open for too long, prompts the most basic question - what should a company or an end user do by the time a patch is available, next to logically switching to an alternative browser? Get back to the basics, and assume the worst in an attempt to mitigate the highest percentage of risk posed by the situation.

Go through related posts: [Secunia: Average insecure program per PC rate remains high](#) ; [Research: 80% of Web users running unpatched versions of Flash/Acrobat](#) ; [Report: 48% of 22 million scanned computers infected with malware](#) ; [Report: Malicious PDF files comprised 80 percent of all exploits for 2009](#)

Calls for "[dropping your rights](#) " have been made for years. And whereas the process has become easier to

implement in the latest versions of Windows, certain companies and end users remain reluctant to implement this basic security auditing process, largely basing their decisions on their obsession with perimeter defense.

[Prevention is better than the cure](#) , even from a cost-effective perspective. There's also no shortage of alternative solutions, such as for instance sandboxing your favorite browser -- [Sandboxie is free for personal use](#) -- in order to ensure that what happens in the sandbox, stays in the sandbox. A similar advice was given by the [American Bankers' Association \(ABA\)](#) last month.

Moreover, in respect to [BeyondTrust's report](#) , there are two fundamental points that the report isn't emphasizing on:

Cybercrime is not driven by the use of zero day flaws, but by the millions of people using the Internet with outdated software - It's a simple fact that has so far contributed to the rise and rise of some of the most prolific botnets, and outdated flaws within popular applications remain the main vehicle for Zeus crimeware infections. Naturally, there are [campaigns that exclusively rely on recently published flaws](#) , but the window of opportunity offered by those would be closed sooner than the one of all the outdated applications running on the same PC, combined. It's the cybercriminal's mentality of traffic optimization for malicious purposes, (See example: [Money Mule Recruitment Campaign Serving Adobe/Client-Side Exploits](#)), that offers the highest probability of infection.

Microsoft OS/software specific vulnerabilities are only a part of the drive-by exploits cocktail served by web malware exploitation kits - You would be surprised to know how many people are so obsessed with "Patch Tuesday" that they exclude the decent number of outdated browser plugins and third-party software installed on their PCs. The result? A false feeling of security, which combined with an outdated situational awareness on how modern web malware exploitation kits work, leads to a successful drive-by attack. It shouldn't come to as a surprise that, not only did [malicious PDF files comprise 80 percent of all exploits for 2009](#) , but also,

[the use of Microsoft Office files for targeted attacks](#) is declining. Two years ago, Microsoft in fact confirmed this trend - [Microsoft: Third party apps killing our security](#).

In terms of closing the window of opportunity that malicious attackers systematically exploit until a patch is released, the best advice is the most pragmatic one. And in this case, it's the easiest one to implement - remove admin rights, sandbox your browser, and [take care of all those third-party apps](#) and [browser plugins](#) .

Report: 48% of 22 million scanned computers infected with malware | ZDNet

The recently released [APWG Phishing Activity Trends Report for Q3 of 2009](#), details record highs in multiple phishing vectors, but also offers an interesting observation on desktop crimeware infections.

According to the report, the overall number of infected computers (page 10) used in the sample decreased compared to previous quarters, however, 48.35% of the 22,754,847 scanned computers remain infected with malware.

And despite that the [crimeware/banking trojans](#) infections slightly decreased from Q2, over a million and a half computers were infected.

More details:

"Though the scanning system checks for many different kinds of potentially unwanted software, for this report, Panda Labs has segmented out 'Downloaders' and 'Banking Trojans/Password Stealers' as they are most often associated with financial crimes such as automated phishing schemes.

The proportion of infected computers detected has decreased for the first time in 2009. In the same way, the proportion of banking Trojans has decreased from a 16.94 percent in Q2 to 15.89 percent in Q3. The proportion of Downloaders has dropped to 8.39 percent from 11.44 percent in Q2 ? but it is still higher than in Q1 (4.22%)."

With the sample itself limited to that of a particular vendor, the remaining over million and a half crimeware infected computers, remain a cause for concern.

Related posts: [Modern banker malware undermines two-factor authentication](#) ; [Citizens Financial sued for insufficient E-Banking security](#) ; [Commonwealth fined \\$100k for not mandating antivirus software](#) ; [Standardizing the Money Mule](#)

Recruitment Process - learn how money mule recruitment works in order to avoid it

Due to its mass adoption, and lack of awareness building on its actual applicability in fighting today's crimeware, two-factor authentication is still perceived as highly effective authentication solution. Otherwise, why would financial institutions keep insisting on its usefulness? Things are thankfully heading in the right direction.

Last month, [a Gartner report](#) (now available for free) discussed the problem, and reasonably stated that two-factor authentication as well as out-of-band communication protocols such as phone verification, fail to protect the customer.

[How does this happen, and how are cybercriminals bypassing the phone verification process?](#)

Malware sits inside a user's browser and waits for the user to log into a bank. During login, the malware copies the user's ID, password and OTP, sends them to the attacker and stops the browser from sending the login request to the bank's website, telling the user that the service is "temporarily unavailable." The fraudster immediately uses the user ID, password and OTP to log in and drain the user's accounts.

Other malware overwrites transactions sent by a user ([URLZone Trojan Network](#)) to the online banking website with the criminal's own transactions. This overwrite happens behind the scenes so that the user does not see the revised transaction values. Similarly, many online banks will then communicate back to the user's browser the transaction details that need to be confirmed by the user with an OTP entry, but the malware will change the values seen by the user back to what the user originally entered. This way, neither the user nor the bank realizes that the data sent to the bank has been altered. Authentication that depends on out-of-band authentication using voice telephony is circumvented by a simple technique whereby [the fraudster asks the phone carrier to forward](#) the legitimate user's phone [calls to the fraudster's phone](#) . The fraudster simply tells the carrier the original phone number is having difficulty and needs the calls forwarded, and the carrier does not sufficiently verify the requestor's identity before executing the fraudster's request.

Last month, [The American Bankers' Association \(ABA\) issued a similar warning](#) to small businesses, recommending the use of dedicated PC for their E-banking activities, one which is never used to read email or visit web sites in an attempt to limit the possibility of crimeware infection.

No matter which adaptive approach you'd consider ([Time to ditch Windows for online banking and shopping](#) ; [Live CDs](#)), cybercriminals have clearly adapted to the currently implemented multi-factor authentication processes in place.

Report: 3 million malvertising impressions served per day | ZDNet

[According to data released by Dasient](#), the company observed a 100 percent increase in malvertising attacks from Q3 to Q4 2010, from 1.5 million malvertising impressions per day in Q3 2010 to 3 million malicious impressions in Q4.

Some highlights from the report:

The average lifetime of a malvertising campaign has dropped for the second consecutive quarter in a row -- down to an average of 9.8 days, as compared to 11.1 in Q3, and 11.8 in Q2.

Malvertisers typically mount their attacks on weekends, during which IT departments are slower to respond, as we have seen in previous quarters, and continued to see in Q4 2010 as per the figure below.

Over the past year, we've estimated that over 4 millions domains have been infected.

After three months of web browsing, the probability that an average Internet user will hit an infected page is approximately 95%.

Cybercriminals usually engage in malvertising attacks in situations where they cannot obtain compromised access to high value, high trafficked web sites. By relying on social engineering techniques to trick major ad networks into serving their malicious content, they get the multi-million impressions exposure that they're looking to get.

It's the higher click-through rate achieved that matters, with the ads appearing on trusted and high trafficked web sites. In some cases, the click-through rate from even a short-lived campaign can outpace, the click-through rate from a well coordinate blackhat SEO (search engine optimization) campaign.

According to Dasient, the malicious attackers usually rely on remnant advertising, that is advertising inventory which isn't sold until the last minute, and work typically on the weekends, with the idea to increase the average time it would take for an IT department to take down the malvertising campaign. [Similar studies](#)

[conducted by Google](#) indicate that the most typical content served is fake security software also known as scareware.

Users are advised to browse the Web in a [sandboxed environment](#), using [least privilege accounts](#), [NoScript for Firefox](#), and ensuring that they are [free of client-side exploitable flaws](#).

See also: [Research: 1.3 million malicious ads viewed daily](#).

'Remove Facebook Timeline' themed scam circulating on Facebook | ZDNet

According to InsideFacebook, scammers are exploiting the negative sentiments surrounding Facebook's Timeline, and are currently spamvertising bogus pages attempting to trick end users into removing their Timeline profile.

[More from InsideFacebook.com](#)

We have found 16 Timeline-related scam pages, which have collectively gained more than 71,000 likes. The largest, with nearly 19,000 likes, has been around for at least two weeks. These pages are among the top search results when searching Facebook for "timeline."

Once the user clicks on on "Continue" or "Like" button, they will automatically become victims of clickjacking/likejacking attempt, and will spread the bogus link on their personal Walls. What the scammers are forgetting is that once the user starts using the Facebook Timeline, there's no turning back no the old profile view.

Users are advised to take advantage of [Firefox's NoScript](#) extension in order to prevent clickjacking and likejacking attempts.

Remote code execution through Intel CPU bugs | ZDNet

[Kris Kaspersky](#) , author of numerous books on reverse engineering and software engineering, will be presenting his

research on [remote code execution through Intel CPU bugs](#) at the upcoming Hack in the Box Security Conference in Malaysia. If his proof of concept code consisting of JavaScript or TCP/IP packet attacks on Intel based machines succeeds, given [Intel's dominant market share on the market](#) the potential outbreak could be enormous since as he claims, the PoC is OS independent, namely all operating systems running Intel chips are said to be vulnerable. Here's an abstract from his upcoming presentation :

"Intel CPUs have exploitable bugs which are vulnerable to both local and remote attacks which works against any OS regardless of the patches applied or the applications which are running. In this presentation, I will share with the participants the finding of my CPU malware detection research which was funded by Endeavor Security. I will also present to the participants my improved POC code and will show participants how it's possible to make an attack via JavaScript code or just TCP/IP packets storms against Intel based machine. Some of the bugs that will be shown are exploitable via common instruction sequences and by knowing the mechanics behind certain JIT Java-compilers, attackers can force the compiler to do what they want (for example: short nested loops lead to system crashes on many CPUs). I will also share with the participants my experience in data recovery and how CPU bugs have actually contributed in damaging our hard drives without our knowledge. "

[Intel will be keeping an eye on his upcoming research](#) :

"George Alfs, a spokesman for Intel, said he has not yet seen Kaspersky's research, nor has he spoken to him about it. "We have evaluation teams always looking at issues. We'll certainly take a look at this one," said Alfs. "All chips have errata, and there could be an

issue that needs to be checked. Possibly. We'd have to investigate his paper."

BIOS based rootkits are nothing new with John Heasman's research into [Implementing and Detecting a PCI Rootkit](#) , published in 2006. And with the possibility of malware hiding at the lowest possible level already a fact, what will be very interesting to monitor is a universal remote code execution based on chip's manufacturer. Everything is possible, the impossible just takes a little longer.

Remote code execution exploit for Green Dam in the wild | ZDNet

The recently exposed as vulnerable to trivial remotely exploitable flaws Chinese censorware Green Dam, has silently patched the security flaws ([China confirms security flaws in Green Dam, rushes to release a patch](#)) outlined in the [original analysis detailing the vulnerabilities](#) .

However, not only is the latest Green Dam v3.17 version still vulnerable to remotely exploitable flaws, but also, for over a week now a working zero day exploit ([Exploit.GreenDam!IK;W32/GreenDam.A](#)) has been circulating [in the wild](#) .

Here are more details on the [remote code execution flaw in the latest version](#) :

"Green Dam intercepts Internet traffic using a library called SurfGd.dll. Even after the security patch, SurfGd.dll uses a fixed-length buffer to process web site requests, and malicious web sites can still overrun this buffer to take control of execution. The program now checks the lengths of the URL and the individual HTTP request headers, but the sum of the lengths is erroneously allowed to be greater than the size of the buffer. An attacker can compromise the new version by using both a very long URL and a very long "Host" HTTP header. The pre-update version 3.17, which we examined in our original report, is also susceptible to this attack."

According to [Green Dam's official web site](#) , the latest 3.17 version which still remains exploitable, has already been downloaded 426,138 times, combined with raw data on over [7,172,500](#) downloads of the previously vulnerable version, the current situation could easily turn the "Great Botnet of China" from theory into practice if the exploits ends up embedded within a web malware exploitation kit.

Remote code execution exploit for Firefox 3.5 in the wild | ZDNet

A [zero day exploit](#) (Firefox 3.5 Heap Spray Vulnerability) affecting [Mozilla's latest Firefox release](#) has been published in the wild. Through an error in the processing of JavaScript code in 'font tags' malicious attackers could achieve arbitrary code execution and install malware on the affected hosts.

There's no indication of its use on a global scale just yet, however due to the fact that the PoC is now public, it shouldn't take long before cybercriminals embed it within the diverse exploits set of their web malware exploitation kits, allowing it to scale.

More details on the mitigation and [the exploit itself](#) :

"Mozilla Firefox is prone to a remote code-execution vulnerability. Successful exploits may allow an attacker to execute arbitrary code in the context of the user running the affected application. Failed attempts will likely result in denial-of-service conditions. The issue affects Firefox 3.5; other versions may also be vulnerable.

NOTE: Remote code execution was confirmed in Firefox 3.5 running on Microsoft Windows XP SP2. A crash was observed in Firefox 3.5 on Windows XP SP3."

Additional testing courtesy of [heise Security](#) indicates the exploit crashed Firefox under Vista, and that when tested under Windows 7 RC1 a dialog abortion script appeared.

In terms of mitigation, [NoScript](#) works like charm, successfully detecting the PoC's attempt to access **file://** .

Redmond Magazine Successfully SQL Injected by Chinese Hacktivists | ZDNet

Irony at its best. It appears that [Redmond - The Independent Voice of the Microsoft IT Community](#) , formerly known as [Microsoft Certified Professional Magazine](#) is currently flagged as a badware site, and third-party exploit detection tools are also detecting internal pages as exploit hosting ones, in this particular case Mal/Badsrc-A. What is Mal/Badsrc-A? Mal/Badsrc-A is a malicious web page also known as HTML.XORER, that has been compromised to load a script from a malicious website.

Redmond's site is part of yet another massive and naturally automated SQL injection attack, whose main malicious URL appears to be down when last checked. Who's behind it, and was Redmond's magazine targeted on purposes? Chinese hacktivists attempting to SQL inject as many sites as possible seem to have come across Redmond's site with no specific intention to do so, comment spammed it, and left a message on the malicious domain (**wowyeye.cn**) which is descriptive enough to speak for itself:

"The invasion can not control bulk!!!!If the wrong target. Please forgive! Sorry if you are a hacker. send email to kiss117276@163.com my name is lonely-shadow TALK WITH ME! china is great! f**k france! f**k CNN! f**k ! HACKER have matherland!"

Two more related sites are affected as well, namely, [Redmond Developer News](#) and [Redmond Channel Partner Online](#) . To bottom line - despite that **wowyeye.cn/ m.js** is currently down, it managed to get injected at 49,900 sites, which like the majority of sites that were participating in the most recent tidal wave of successful SQL injection attacks, continue to remain vulnerable to copycats introducing new malicious domains within the vulnerable sites.

It is also important to emphasize on the fact that this is a lone gunman operation, and not necessarily one backed up by [a botnet such as Asprox](#) , which got some publicity for its involvement in

automated SQL injections attacks. Whether or not [a standalone SQL injecting tool](#) was used (screenshots included), the concept of [using botnets which would create their hitlists from public search engines' indexes](#) (screenshots included) and automatically SQL inject or [Remotely File Include](#) them, has been around for years with the availability of such scanning modules available for the botnet masters to take advantage of.

And now that the probability of locating and successfully exploiting vulnerable sites is increasing due to the success rate of previous campaigns, what we would be dealing with for the next couple of months are [the copycats](#) who just memorized a new buzz word -- SQL injection -- and efficiently execute massive unethical web applications pen-testing all over the Web.

Q&A of the Week: 'The current state of the cybercrime ecosystem' featuring Mikko Hypponen | ZDNet

In this week's Q&A of the Week, I chat with [Mikko Hypponen](#), the Chief Research Officer of F-Secure. His [TED Talk on computer security](#) has been seen by almost a million people and it has been translated to over 35 languages.

We discuss the recent botnet take downs, OPSEC (operational security) within the cybercrime ecosystem in a post-DarkMarket world, the rise of the cybercrime-as-a-service business model, as well as current and emerging mobile malware trends.

Go through the Q&A, and don't forget to TalkBack.

Dancho: From [Kelihos](#) , [Rustock](#) , [Waledac](#) , to the successful [extraction of 33GB of raw crimeware data back in 2010](#) , and the most recent violation of OPSEC (operational security) where a botnet master offered [insights into his malicious operation on Reddit](#) , do you think that over the past couple of years cybercriminals have failed to properly apply the OPSEC approach to their campaigns and infrastructure, potentially allowing security researchers and vendors an easier way to take down their campaigns? What are some of your most recent observations regarding the OPSEC applied, or the lack of OPSEC applied to cybercrime campaigns?

Mikko: There still are online criminals who are looking for attention. They want somebody to notice how clever they are. That's why they post on forums. That's why they are on Reddit and Twitter. That's why they are still sending messages to their enemies in texts embedded inside malware code. And when we move from financially-motivated attacks to the world of movements like Anonymous, OPSEC violations are everywhere. For the most part, it's trivial to monitor the movements of groups like these, as they communicate in the open.

Dancho: From encrypted instant messaging communications, VPN service providers, to invite-only web forums, cybercriminals are increasingly becoming aware that they're being watched. How would you describe the cybercrime ecosystem in a [post-DarkMarket world](#) in terms of the growth of underground communities, increasing number of market participants, and a growing number of highly diversified underground market propositions by dedicated and highly professional vendors of the service? Have we witnessed the development of a multiplying effect resulting in dozens of newly launched communities with better OPSEC (operational security) compared to the DarkMarket, or are we basically seeing amateur copycats attempting to achieve notoriety within the cybercrime ecosystem?

Mikko: The most important movement is that many of the traditional marketplaces are moving from the traditional web to the deep web, via services like Tor and Freenet. This makes them much more anonymous and much harder to track. In my discussion with law enforcement, they clearly worry about this a lot. In the deep web, it's easy to find all kinds of illegal content - from credit card sales to botnets to DDoS to public sales of drugs all the way to apparent hitmans. Some of them are surely scams.

I believe vast majority (if not all) of the deep web hitmans will just take your money and run. A major part of the deep web is illegal content. That's exactly why they don't want to have their stuff in the public web. But criminals get caught even if they host there. This is what happened to the "Farmer's Market" drug trading site in the deep web.

Dancho: It's a public secret that, in order for a law enforcement agent or a security researcher interested in maintaining their access to an invite-only cybercrime-friendly forum, they would need to get involved in the actual trade of fraudulent goods and services inside the forum. Do you believe that on its way to catch the forum administrators, law enforcement actually gave novice cybercriminals the opportunity to socialize and gain 'know-how'? Can we quantify

the prevented losses by catching the forum administrators, in between quantifying the losses out of the active socializing and networking of the novice cybercriminals that took place?

Mikko: I've maintained a set of identities across various forums for years and years without engaging to actual trade of fraudulent goods. It can be done. For a newcomer, that might be very hard to achieve, but if you have a history, it can be done.

Dancho: Do you see the actual applicability of the DarkMarket take down, or was it just an over-hyped take down taking into consideration the fact that the DarkMarket forum is just the tip of the iceberg when it comes to the number and quality of competing underground communities?

Mikko: DarkMarket takedown was important in many ways, even though it obviously did not stop the actual problem.

Dancho: Over the past few years, we've witnesses the tremendous growth of cybercrime-as-a-service underground market propositions. Years ago, a novice cybercriminal would need to posses certain technical knowledge, or at least have the right contacts. Nowadays, everything from [spam](#) , [phishing](#) to launching malware attacks and [coding](#) custom [malware](#) is available as a service. Do you believe the community somehow made a mistake by allowing the cybercrime ecosystem to scale to the point of industrial [standardization of the services](#) and products offered? What was that mistake, and what can we, as a security community do to undermine the effectiveness of this underground market concept known as scalability?

Mikko: I don't see how we could have prevented this. These are not technological problems; they are mostly social problems. And social problems are always hard to fix. Having said that, it's sobering to see just how specialized cybercrime-as-a-service have become. It's not just enough that criminals are selling hosting and spamming or botnets to each other.

Some criminals are sellings banking trojans and then other hackers are selling tailor-made configuration files for those trojans, targeting any particular bank. Going prices for such config customization seem to be around \$500 at the moment.

Dancho: Next to cybercrime-as-a-service proposition, [affiliate networks](#) truly allowed the cybercrime ecosystem to scale, now that there was an efficient and market-sound way for cybercriminals to monetize their activities. Do you believe that as a concept affiliate networks are more important to the overall growth of the cybercrime ecosystem, or was it cybercrime-as-a-service propositions that allowed it grow at such an alarming rate?

Mikko: The "Partnerka" affiliate networks behind rogue AVs and ransom trojans were so succesful that they really changed the landscape. Affiliate model also provides some protection to the masters behind the schemes, as they don't need to get their hands dirty anymore.

Dancho: We've been seeing quite a lot of attacks targeting Mac OS X lately. Flashback was a game-changer in terms of infected hosts. We've even seen [Mac OS X based ransomware](#) experiments being conducted next to working copies of [scareware variants](#) running on Mac OS X. However,these attacks are not reaching the epidemic growth of malware attacks targeting Microsoft's Windows OS. Personally, I believe that we're not seeing an epidemic growth of Mac OS X malware due to the lack of an affiliate network monetizing Mac OS X infected hosts? Do you believe that's the case, why and why not?

Mikko: Historically, Flashback.K outbreak is very important. Just a month ago, the general guidance was that you didn't really need an antivirus for your Mac. Now you do. At it's peak, somewhere between 2% to 5% of all the OS X machines on the planet were infected. That's huge. However, that's just one case. We are not seeing a wave of Mac malware. We're seeing one successful gang going at it.

Dancho: Every then and now, in an attempt to raise more awareness on the growth and the impact of cybercrime, the mainstream media compares the revenues from cybercrime to the revenues earned from drug trade. Do you believe that cybercrime is more profitable than drug trade?

Mikko: No, it's not. Can't be.

Dancho: Also do you believe we now possess mature and scientific approaches to accurately quantify the revenues earned and lost in both of these markets?

Mikko: We don't. I think the most interesting number would be how much online crime is generating profits to the criminals - ie. how much are they pocketing. Obviously the losses they generate are far higher. But the actual earnings would be really interesting to know. And we don't - except in isolated cases. We do know of individual groups which have made tens of millions of dollars. But not hundreds.

Dancho: The majority of end and corporate users still live in a "Patch Tuesday" reality, where they believe that vulnerabilities found in Microsoft's products still dominate the threat landscape, and that this is exactly what the cybercriminals are exploiting. However, that's no longer the case. These days, the [majority of vulnerabilities are found in third-party applications and browser plugins](#) .

Cybercriminals are naturally quick to follow, by embedding these very same flaws in their web malware exploitation kits. Do you believe that the security community should do a better job in building awareness among end and corporate users by alerting them on the current practice of exploiting flaws in third-party software and browser plugins, compared to exploiting flaws related to Microsoft's products in general? For instance, [Mozilla's Plugin Check](#) is a great initiative. Do you believe it deserves more visibility? Has the time come for search and social networking giants to start embedding this feature within their interfaces in an attempt to better protect millions of end and corporate users?

Mikko: In the Windows world, drive-by-downloads via exploits targeting browser add-ons and plugins are clearly the most common way of getting infected. That's why anything we could do to improve patching (or disabling) of vulnerable extensions would really make a difference. Mozilla's initiative is great, but in practice the Chrome model of sandboxing and replacing third-party add-ons with their own replacements seems to work really well.

We can see this when we look at real-world data from the statistics of exploit kits: Chrome users get exploited less than Firefox or IE users. Which is great news, as Chrome is about to become the most common browser on the planet. Chrome might have privacy issues, but from technical security viewpoint, it's pretty good.

Go through previous Q&As:

[Q&A of the Week - 'The current state of the crimeware threat' featuring Thorsten Holz](#) **[Q&A of the Week: 'The current state of the cyber warfare threat' featuring Jeffrey Carr](#)**

Dancho: Over the past couple of years, we've witness the rise of the so called '**[Opt-in botnets](#)** ' where patriotic hacktivists -- often average Internet users -- on purposely infect themselves with agents distributed in an attempt to gain control of their bandwidth for launching distributed denial of service attacks (DDoS) against a particular target, or do it by themselves thanks to the publicly obtainable DoS and DDoS attack tools.

First pioneered by China as the "**[People's Information Warfare](#)** " concept, it has been pretty popular in each and every cyber conflict we've seen over the past couple of years. Were you surprised when you first witnessed it in action in the context of actual impact it had on the targets? Do you believe 'Opt-in' botnets are the future, or are we going to see hybrid attacks consisting of both, end users who 'opted-in' in combination with DDoS bandwidth offered by good old fashioned botnets? Is this a trend, or a fad?

Mikko: I really dislike DDoS as a concept and I wish we wouldn't have to fight this problem any more in 2012. But we do, and it's likely to stay with us forever. Akamai has already reported seeing DDoS attacks launched from a botnet of mobile phones. We're likely to see DDoS botnets move to totally new platforms in the future. Think cars and microwave ovens launching attacks. Tools as LOIC and HOIC have brought the "Opt-in botnet" model to the masses, and it works. Unfortunately.

Dancho: Iran has recently announced that it's banning the import of foreign security software, and that **[it has been secretly working on its own antivirus software](#)** . Taking into

consideration the fact that the majority of antivirus solution also detect DoS and DDoS attack tools distributed in an event of a cyber conflict, do you believe that Iran is setting up for the foundations for successful hacktivist attacks in the long term, given the fact that it could on purposely not detect the attack tools distributed to its netizens?

From a strategic perspective, is this in-house patriotic sentiments driven move a step in the right direction, or is the country potentially exposing its entire Internet infrastructure to attacks from malware authors that would now only need to bypass a single antivirus product, Iran's own security solution?

Mikko: I'll skip this question as I didn't even know Iran has announced that. But as a side note, have you seen this? <http://av.0days.ir>

Dancho: Mobile malware is growing at an exponential rate, with the cybercriminals behind these campaigns clearly "thinking market share". In the past, we've also seen [malware systematically bypassing Symbian's code signing procedure](#), potentially compromising the trust of end and corporate users. We're also currently seeing the systematic abuse of legitimate app marketplaces, with cybercriminals successfully using them for distributing malicious software. Which are the most commonly targeted mobile operating system?

Mikko: As our latest [Mobile Threat Report](#) shows, Android has made malware for Linux a reality. Old Symbian malware is going away. Nobody is targeting Windows Phone. Nobody is targeting iPhone. And Android is getting targeted more and more. iOS, the operating system in iPhone (and iPad and iPod) was released with the iPhone in the summer of 2007 - five years ago. The system has been targeted by attacker for five years, with no success. We still haven't seen a single real-world malware attack against the iPhone. This is a great accomplishment and we really have to give credit to Apple for a job well done. Out of all Linux variants, Android is the clear leader in malware.

Dancho: Mobile payments (a.k.a micro payments) are gaining a lot of popularity. Now that we've seen [a Zeus crimeware](#)

variant targeting mobile operating systems , do you believe that this is the next frontier for mobile malware authors in comparison to the low-revenue earning fraudulent techniques where mobile malware-infected devices would send SMS message to premium rate number, or a ransomware requesting a micro-payment for unlocking the device? Is the mobile payments industry ready to fight mobile banking malware, or is it currently lacking behind in truly understanding the dynamics of the threat?

Mikko: I believe the near-future mobile malware will be cashing out by sending text messages and placing calls to expensive premium-rate numbers. It works and it's easy to do. Eventually, we'll probably see more mobile banking trojans and new trojans targeting micropayments.

Dancho: On a periodic basis, the security community intercepts a malicious attack targeting **human rights activists** and their supporters. These **targeted attacks** against the organization's employees and supporters are becoming increasingly common. What are some of the latest trends you're observing in this field? Do you believe that we're ever going to properly attribute the source for these attacks, behind the obvious common sense applied by the researchers profiling them?

Mikko: Attribution is not problematic here: it's the Chinese. Proving that is hard though. We've also been able to link some of these targeted attacks against human rights organizations and minority support groups to attacks targeting huge defence contractors and governments, proving that they we're coming from the same source.

Dancho: In an attempt to trick web reputation filters, cybercriminals are increasingly relying on **legitimate infrastructure** for **launching their campaigns** , and actually hosting the command and control servers inside the cloud. From Facebook, to **Twitter** , **Amazon's EC2** , **LinkedIn** , **Baidu** , Blogspot and Google Groups, each of these services have been abused by cybercriminals in the past. Do you believe this is a trend or a fad?

Mikko: Professionally run services like Amazon or Facebook will kick out abusers like this fairly quickly, forcing them to host their stuff on more crime-friendly network.

Dancho: How would you comment on the recent [SOCA/FBI operation that took down 36 criminal credit card stores](#) ? A job well down, or a drop in the bucket taking into consideration the fact that a significant number of the carder web sites that I exposed and profiled in 2011, remain active, sometimes just responding to a periodically changed domain?

Mikko: What else are they supposed to do? They do their best in trying to go after at least some of these guys and we should commend them on that - even if it wouldn't really change the big picture by much.

Dancho: What do you think South Korea's proposed '[Zombie PC Prevention Bill](#)' making security software mandatory on all users' PCs? Should other countries also follow this example? A report published in 2011,for instance, indicated that even PCs with antivirus software running on them, were still getting infected with malware? How would you comment?

Mikko: I believe in giving people the freedom to use their computers as their wish. However, I also like giving strong guidance to users who don't really know what they should be doing. I believe operators are in a key position to move security from a product to service and to protect the masses with both managed security solutions on end-user devices as well as behind-the-scenes monitoring and filtering of malicious traffic.

Dancho: In March, 2011 [I proposed that all ISPs should quarantine their malware infected users](#) until they prove they can use the Internet in as safe manner, by taking care of their information security flaws. Do you think this is a good idea? Why and why not? Has the time for ISPs to start at least alerting users that they're infected with malware, in between raising awareness on the long-term and short-term consequences of that infection?

Mikko: I love this idea and we are successfully doing this with our solutions together with several operators. It works.

Dancho: The [Carberp Trojan case](#) attracted the media attention as among the few examples where Russian law enforcement actually did its job. From a strategic perspective, do you believe that the cybercrime gang behind the campaigns made a mistake by targeting Russian users, thus attracting the attention of Russian law enforcement?

Mikko: We believe they got greedy, and made the wrong people angry. They were making significant profits partly by building complicated networks of packet mules, keyloggers and local proxies to make fraudulent purchases of electronics in online stores. These goods ended up being resold to buyers at far below the market value. Such actions get detected fairly easily.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Q&A of the week: 'The current state of the cyber warfare threat' featuring Jeffrey Carr | ZDNet

Dear blog readers,

ZDNet's Zero Day begins a new weekly feature called 'Q&A of the Week' which aims to bring you invaluable insights from industry leaders and internationally recognized experts in the areas of cybersecurity, cybercrime and cyber warfare.

In the first post of its series, I chat with [Jeffrey Carr](#), a cybersecurity expert and author of '[Inside Cyber Warfare: Mapping the Cyber Underworld](#)', on the current state of the cyber warfare threat.

We discuss Stuxnet, Russia, China, Iran, cyber conflicts, false-flag operations, and the U.S's current understanding or lack of understanding of its adversaries' true cyber-warfare capabilities.

Enjoy and don't forget to TalkBack, we'd love to hear from you!

Let's start from the basics. Who is [Jeffrey Carr](#)?

Jeffrey Carr, the founder and CEO of Taia Global, is the author of "Inside Cyber Warfare: Mapping the Cyber Underworld" (O'Reilly Media 2009 and 2011 (2nd edition)). His book has been endorsed by General Chilton, former Commander USSTRATCOM and the Forward to the Second Edition was written by former Homeland Secretary Michael Chertoff. Jeffrey has had the privilege of speaking at the US Army War College, Air Force Institute of Technology, Chief of Naval Operations Strategic Study Group, the Defense Intelligence Agency, the CIA's Open Source Center and at over 60 other conferences and seminars.

Now that you know more about Jeffrey, here's the actual conversation.

Dancho: Nowadays, the mainstream media often portrays cyber attacks using the term "*Digital Pearl Harbor*"? Do you believe that a devastating attack on U.S infrastructure must take

place for policy makers and the general public to start paying more attention to the ongoing cyber-warfare arms race? Also, do you believe that the focus on a devastating attack has shifted the attention from the current threat landscape where cyber spies from multiple governments systematically penetrate and steal intellectual property from Fortune 500 companies?

Jeffrey: No, I don't think a major catastrophe is necessary. We're already at a point where cyber security is being taken more seriously due to the vast amount of IP theft. That's not to say that we're doing the right things because we aren't. But the awareness of the problem and the desire to do something about it both currently exist sans any type of digital Pearl Harbor.

Dancho: How significant is the role of mainstream media to raise awareness on the current situation, and do you believe it has the knowledge and understanding of the problem to do so?

Jeffrey: Media is critical in raising awareness but 99% of journalists don't have the requisite knowledge to report the story accurately.

Dancho: How would you describe [Iran's current understanding of information warfare operations](#) , and overall cyber-warfare ambitions? Do you believe Iran is a threat, based on the relatively modest hacking activities we've seen by pro-Iranian hacktivists, or are they on purposely not revealing the true state of their cyber warfare capabilities in order to misinform the public and U.S policy makers?

Jeffrey: I believe that Iran should be taken seriously as a State with aggressively developed cyber-warfare capabilities. Iran's Islamic Revolutionary Guard Corps set up its first official cyber-warfare division in 2010 with an estimated budget of US\$76 million. There is also an Iranian cyber militia that is supposed to number about one million persons. Some of their hacker crews have demonstrated a high degree of skill in past attacks against Israeli government sites and [China's Baidu.com](#) - and at least one crew is known to be connected with the Iranian government.

Dancho: Can you compare Russia vs China in terms of operational capabilities and intent to launch cyber attacks, which of these countries is more persistent, and what is the overall difference in their cyber-warfare doctrines, if any?

Jeffrey: Yes, both Russia and China are spending a lot of money on encouraging foreign investment within their borders which in turn allows their security services to capture a vast amount of proprietary information in three ways: (1) via normal communication channels (satellite, landline, mobile, VPN, etc.); (2) through technology transfer which occurs when Russian and Chinese engineers are hired to work at foreign companies for 1-2 years and then transfer to State-owned companies - +taking the knowledge that they learned with them; and (3) by their respective security services, approaching foreign companies and demanding copies of their source code for national security reasons. All three of these strategies are perfectly legal and don't require hacking into a network. Having said that, both countries also acquire stolen IP from professional hacker crews of mixed nationalities.

And both countries have stood up information warfare units (neither country uses officially uses the term "cyber") but only Russia has combined kinetic attacks against foreign countries with a cyber component (i.e., Georgia, Kyrgyzstan, and Chechnya). China has not used its cyber capabilities in an offensive way - at least not as far as I've seen.

Dancho: Collectivist societies such as Russian and China have a stronger and more vibrant civilian cyber militias , compared to individualistic societies. Do you agree, or disagree and why? Also, do you believe that Russia and China are "subverting the enemy without fighting him", by forwarding the process to their collectivism-minded civilian or government-tolerated cyber warriors ?

Jeffrey: I believe that Estonia is organizing a cyber militia and they're a democratic society. I think the U.S. would have some success at that as well if the DOD ever agreed to set it up. Many countries, including the U.S., Israel, Russia and China, engage in information warfare and influence operations which include a cyber

component. However, Russia won't hesitate to use an iron fist where China will find ways to exert pressure in more subtle ways.

Dancho: While the [Pentagon is busy drafting](#) cyber warfare rules of engagement, Russia and China are busy allowing the development of [self-mobilizing civilian cyber militias](#) ? Do you believe the Pentagon is aware of these latest developments, or it's stuck in a "paper tiger" warfare with these nations?

Jeffrey: The Pentagon is certainly aware of those foreign cyber militias. It's not as if it's a secret. I just don't think that the DOD wants such a civilian militia set up in the U.S. unless it's part of the National Guard.

Dancho: Are you aware of the existence of the so called "[People's Information Warfare](#) " concept, originally pioneered by China, as well as the rise of [opt-in botnets](#) where average Internet users knowingly donate their bandwidth and network connectivity for use in ongoing cyber attacks?

Jeffrey: Yes, I think it's a testament to the fierce nationality and patriotism found in many foreign countries. Many citizens naturally want to support their government in times of crisis. For example, most of the cyber attacks done by Chinese hackers against foreign targets were performed after an attack against China (i.e., the Kosovo bombing of China's embassy, the [downing of a Chinese military jet](#), the attack against Baidu, etc.). The Russian cyber attacks against Estonia were launched after the perceived insult of Estonia moving a Russian statue. I'm not siding with either government. I'm simply making the observation that civilians typically involve themselves in group cyber attacks when they believe that they're defending their country.

Dancho: For years China has been developing and promoting the use of its own hardened secure Operating Systems, such as Kylin OS and Red Flag Linux. Europe followed this example with its secure OS Minix, and Russia is also showing interest in the concept of a nation-sponsored secure OS. Taking into consideration the fact that the U.S military has spent years developing offensive cyber warfare weapons affecting Microsoft's Windows, the most widely distributed operating

system globally, does this put the U.S at a strategic disadvantage, or is China actually undermining the security of its own infrastructure by introducing a new, largely untested Operating System for public and military use?

Jeffrey: Well, I'd call it an inconvenience at most. We should have the resources to obtain the source code for those new operating systems in much the same way that our own source code is obtained by foreign agents or hackers. Interestingly, a lot of coding is out-sourced to other countries so the opportunities to "intercept" it are certainly there.

Dancho: Microsoft recently kicked out a Chinese company from its Microsoft Active Protections Program (MAPP) program. However, through its Microsoft's Government Security Program (GSP), the company is [sharing source code with Russia's FSB and the Chinese government](#) . Do you believe this poses a risk to U.S national security, and are the financial benefits out of the deal worth the possible national security implications in the age of Microsoft's mono-cultural dominance?

Jeffrey: Yes, I do see it as a national security threat. In fact, any foreign company that wants to do business in Russia, China, or even India, must surrender their source code upon request of the security services or face the possibility of having their license to do business in that country pulled.

Dancho: It's fairly logical to assume that nations involved in defensive cyber-warfare activities, are also busy pursuing the developing of offensive cyber-warfare weapons. In fact, in the past on numerous occasions the Pentagon has expressed its intentions to use kinetic force against sources of cyber attacks somehow endangering the CIA's (Confidentiality, Integrity and Availability) networks. Are you a firm believer in the applicability of "virtual shock and awe" campaigns in today's interconnected world? How would you comment on the possibility of an adversary using [compromised legitimate infrastructure as a "virtual human shield"](#) in an attempt to undermine the offensive cyber warfare capabilities of a particular nation, the U.S for instance?

Jeffrey: I can only speculate, of course, but I think you pose a reasonable strategy that many nation states are worried about; hence the frequent discussion of drafting treaties that dictate certain Rules of Engagement. Most want to prevent cyber attacks against critical infrastructure or other civilian targets that could cause mass disruption.

Dancho: Government tolerated vs government sponsored cyber attacks? Do you make a difference between the two and just how important is it at the end of the day?

Jeffrey: Both Russia and China "tolerate" certain illegal actions by organized crime groups in exchange for future cooperation from those same groups in matters related to national security. This could certainly include cyber criminals who are affiliated with organized crime. A "sponsored" attack might mean one performed by one of those protected gangs or one done by a patriotic organization such as the official state-run youth associations in Russia or large patriotic hacker organizations like the Red Hacker Alliance in China. I think it's important to understand that these states have multiple resources to draw from before they get to the third option - using their in-house capabilities; i.e., their foreign intelligence services.

Dancho: The Russia vs Estonia cyber attacks are often described as "World Web War I"? Do you believe this is the case, why and why not?

Jeffrey: No, not at all. It certainly wasn't the first time that Russia mounted cyber attacks against another State. They did it at least twice before in 2002 (Chechnya) and 2005 (Kyrgyzstan). Chinese hackers mounted thousands of attacks against U.S. government websites in 1999 after the accidental NATO bombing of the Chinese embassy in Kosovo.

Go through a previous Q&A conversation - [The current state of the crimeware threat](#)

Dancho: In [Russia vs Georgia cyber attacks](#) we saw an example of Russia's understanding of information warfare operations . Do you believe the attackers were government sponsored, or were they basically government tolerated given the lack of prosecution for any of the involved hacktivists and

botnet masters ? Is it important to make the difference between the two cases in the context of cyber attack attribution? Why and why not?

Jeffrey: I believe that there was government direction involved in the cyber attacks mounted against Georgia, and that this direction was funneled through the State office that runs the Nashi. I'm confident that Nashi leadership received their instructions from highly placed Russian officials and passed it to their membership who in turn organized their attacks via online forums like **StopGeorgia.ru** . Most of the research that I've done on the cyber component of the 2008 Russia Georgia war can be found in my book "Inside Cyber Warfare" and in the Project Grey Goose reports (Phase I and II).

Dancho: The discovery of Stuxnet also dubbed the "Nuclear Worm" changed everything. Do you believe this was the first time the security community successfully intercepted a nation-to-nation cyber black ops operation?

Jeffrey: Yes, Stuxnet was certainly a game-changer in terms of known cyber attacks. There may have been more sophisticated worms out there but Stuxnet was the first of its kind that was made public.

Dancho: Could Stuxnet be described as the revenge of the pro-Western Ph.Ds, or do you believe it had to be a pro-Western government-funded operation to begin with? Also, do you need a Ph.D to launch a cyber operation similar to Stuxnet, or not so technically sophisticated attackers could have achieved the same effect if they wanted to?

Jeffrey: You certainly don't need a Ph.D. to create a worm like Stuxnet. Ralph Langner, who has done much of the heavy lifting around analyzing Stuxnet, doesn't even have an engineering degree. He has a degree in Psychology, I believe, and taught himself engineering later in life. You do need to have a knowledge of industrial control software and an engineering degree would certainly help, but that's about it.

Dancho: In the latest edition of Richard Clarke's book 'Cyber War', he argues that Stuxnet is a virtual boomerang that will eventually hit back the U.S, a country he believes is among the

countries that sponsored and actually executed the attacks. How would you comment?

Jeffrey: Richard Clarke should stick to something he knows about like counter-terrorism and avoid speaking about things which he knows nothing about like cyber warfare or cyber security. I doubt that he can make any kind of case that the U.S. was responsible beyond a wink and a smile. No one wants Iran to have nuclear weapons and that includes Russia and China. The fact that neither country wants Iran to be enriching uranium and that fact that both countries haven't supported sanctions suggests to me that Stuxnet could have come from either of those two countries just as easily as from a Western nation. After all, if not sanctions, why not a worm designed to cause havoc and hopefully dissuade Iran from further enrichment activities?

Dancho: I once pointed out that "[Cybercrime is an element of economic warfare](#)". How would you comment?

Jeffrey: I agree with you. I've also pointed out that cybercrime finances the development of cyber "weapons" which can be used in acts of espionage or geo-political actions like Estonia, Georgia, etc.

Dancho: Malware infected hosts has been used as [stepping stones for launching more cyber attacks](#) , and [hiding the physical location](#) of the [attacker for years](#) . Burkina Faso could easily impersonate Russia, China or Iran online, a scenario we've already seen in Tom Clancy's '[The Sum of all Fears](#) ' . Locked in between all the current cyber warfare tensions, do you think we're missing the possibility of an ingenious anti-Western oriented mastermind or a regime located in a Third World country, pulling the strings behind such campaigns? How realistic do you believe is the potential that developing nation states could be launching false-flag cyber operations in an attempt to engineer cyber-warfare tensions between developed nations?

Jeffrey: I'm not much for "masterminds" but a false-flag operation is a real threat and, in my opinion, it's standard operating procedure to launch an attack from servers that are not in the same geographical region as the attacker.

Dancho: Access to thousands of [geolocated malware-infected hosts](#) could be easily purchased, thanks to the increasing number of underground market propositions offering access to such hosts. With each and every Fortune 500 company reporting a successful cyber intrusion or that they're permanently under attack, just how prevalent do you believe is the collection of valuable [OSINT data through these easy to purchase botnets](#) ?

Jeffrey: My view based on incident response work that my company has done for DIB members and other Fortune 500 companies is that most attacks are done by mercenary hacker crews who in turn sell the valuable data that they've stolen to governments or other interested parties. Those hacker crews most likely utilize cheap botnets whenever they can since it would help obscure any attempt to identify who they are.

Dancho: North Korea is well known to have developed its own cyber-warfare units, for instance, the [infamous "Unit 121"](#) . How would you describe North Korea's current understanding of information warfare operations, its capabilities and intent to launch cyber attacks against the U.S and South Korea?

Jeffrey: North Korea has spent a great deal of money on its IW capabilities. It sends its soldiers to excellent schools in India and China for technical training. If you can believe South Korea, it suffers from multiple successful attacks originating from the North. I haven't seen any evidence of North Korea launching what I would call serious attacks. They seem to be mostly nuisance DDoS or defacement strikes. South Korea has cried "wolf" a bit too much for me to believe everything they say about being the victim of cyber attacks from Unit 121.

Dancho: With its well known ally China, North Korea could easily adopt China's information warfare model in an attempt to gain strategic advantage in future cyber-warfare conflicts. With cybercrime-as-a-service underground market propositions increasing, just how feasible do you believe is a situation where North Korea starts outsourcing all of its cyber warfare needs to Russian or Chinese cyber criminals?

Jeffrey: I doubt that's ever going to happen. The North Korean government is too unstable, too irrational, for either Russia or China to tolerate that situation.

Dancho: North Korea is often given a relatively low score on the infamous [Cyber Threat Matrix](#) estimating the cyber warfare capabilities of multiple nations. However, the same doesn't apply to Russia or China. Do you believe in the relevance of Cyber Threat Matrixes? Do you think that North Korea could easily occupy one of the top positions on these by simply outsourcing its cyber-warfare needs to its ally China, or perhaps even Russia? Should we fear North Korea's in-house cyber-warfare doctrine, or should we feel the day it starts outsourcing in an attempt to catch up with the rest of the world?

Jeffrey: I haven't seen a cyber threat matrix that I have any confidence in. North Korean IW soldiers are well-trained as I said in my answer to one of your previous questions. I wouldn't put them at the top of any list but neither would I put them at the bottom. I think they hold a solid mid-level position.

Dancho: From Eligible Receiver, to Silent Horizon and [Cyber Storm](#) , how would you describe the practical relevance of cyber exercises performed by the U.S in today's fast changing cyber threat landscape? Moreover, how would you describe the OPSEC leak when Cyber Storm's Power Point presentation containing details on the actual cyber warfare scenarios leaked on Cryptome.org in 2006? Do you believe this leak allowed foreign adversaries a peek into the U.S's understanding of cyber warfare, or did it have a minimal impact on the OPSEC of the exercise?

Jeffrey: Leaks are never good from an OPSEC point of view. And other governments closely monitor everything that the U.S. Dept of Defense is doing in cyberspace.

Dancho: From Solar Sunrise, Moonlight Maze, Titan Rain, Operation Shady RAT, the the Night Dragon campaigns, the rise of the so called advanced persistent threats (APTs) is pretty evident. Do you believe that publicly sharing details on

successful cyber-espionage campaigns undermines the confidence of the U.S's allies in the U.S's ability to protect its critical networks, potentially giving its enemies the blueprint to launch similar attacks in the long term?

Jeffrey: Our allies are sometimes the ones responsible for those attacks, Dancho! France, Germany, and Israel are all very active in terms of conducting cyber-espionage operations against corporations. Overall I'm in favor of information sharing as long as the names of the victims are kept confidential. I see no risk to the U.S. in publishing facts about network breaches. No country is safe from those types of attacks.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Q&A of the Week - 'Tales from the Underground' featuring Brian Krebs | ZDNet

The third Q&A part of ZDNet's Zero Day weekly column 'Q&A of the Week', is now a fact.

In the third post of its series, I chat with [Brian Krebs](#), investigative reporter covering cyber security and cybercrime, and currently editor in chief of [KrebsOnSecurity.com](#). We discuss the cybercrime ecosystem, the money mule problem, ATM skimmers, [pharmaceutical affiliate networks](#), and payment processing gateways for the scareware industry.

Enjoy the conversation, and don't forget to TalkBack.

Dancho: ATM skimming is proliferating, next to the overall availability of bank plastic cards, holograms and pretty much everything a carder needs to cash out the fraudulently obtained credit card data. From ATM skimmers with bluetooth notification, to [ATM skimmers with SMS notification](#), what are some of the latest innovations in this field that you're observing?

Brian: One innovation in skimming that I wrote about recently is that [crooks are starting to turn to 3D Printers to make these devices](#). An investigator in California shared with me some photos of what was believed to be a 3D printed skimming device, which was the news hook for that story. But as I was researching the topic, I discovered that a skimmer gang had recently been convicted of creating skimming devices made with a 3D printer they had purchased with the proceeds of their previous skimming crimes.

Dancho: Are cybercriminals a step ahead of the banking industry, and what can the banking industry do to prevent the mass adoption of ATM skimming devices? Is the problem lack of innovation, or lack of implementation of currently available solutions?

Brian: Sure. The crooks are nearly always ahead. But the real problem is not that the technology doesn't exist to cut way down on

this type of fraud; it's that by and large, banks in the United States haven't adopted it. Chip-and-pin is not a panacea to the skimming problem, but it does increase the costs to the fraudsters by making ATM cards more difficult and expensive to counterfeit. Most of Europe is moving toward or has adopted this standard, and yet skimming fraud remains a big problem there. Tellingly, a majority of the skimming losses against European banks happen when skimmed card numbers are sent over to the United States, where they are encoded onto plastic and used to withdraw funds from the accounts using US ATM machines, which do not require chip and pin.

Dancho: In your ['Pharma Wars' series](#) , you've extensively profiled some of the key affiliate networks and payment processors behind the growth of the cybercrime ecosystem. What are some of the current and emerging trends in regard to pharmaceutical affiliate networks? Also, do you believe that pharmaceutical scams are more profitable than scareware and Pay-Per-Install schemes? Why and why not?

Brian: I think there are a few trends emerging, and they all have to do with the fact that it's getting harder for rogue pharmacies to make money. One is a shift toward more generic and herbal medications. The affiliate programs seem to be looking for drugs to sell that don't incur intellectual property violation cases, which can get them shut down in a hurry. But I think it is becoming much harder for the larger volume spam and scareware affiliate programs out there to retain reliable processing, and that's a long overdue but welcome development.

Dancho: The media often portrays a picture where Eastern Europe is the epicenter of the cybercrime epidemic. Do you believe that's still the case, or do you believe that in 2012 cybercrime has spread internationally in a way it can no longer be accounted for in terms of revenue earned and amounts stolen?

Brian: If you mean financially-motivated cybercrime that affects the rest of the world, I would say without question hackers in Russia and Eastern Europe are the most active, if not also the most profitable. I

think there are cases where (dis)organized crime groups have and are conducting a lot of cybercrimes, but many of these sophisticated groups tend to be regional and stick to attacking their own (Brazil is a good example).

But generally speaking I think it is a mistake to try to measure cybercrime by actual losses, which almost never comes close to the real losses and damage done by cybercrime, costs incurred by software and hardware and personnel defenses, etc. Don't get me wrong: I strongly believe that all nations should be working harder to quantify and publish data about cybercrime losses, particularly in the financial sectors. But the reality is that even some of the most active criminal groups -- such as the rogue pharmacy "partnerka" programs like SpamIt and GlavMed and Rx-Promotion -- employed some of the biggest botmasters with the biggest botnets, and while some of them made a lot of money, most did not. And the spam partnerkas are excellent examples of cases where there are huge asymmetries between their earnings for these activities and the tens of billions of dollars companies and individuals need to spend each year to try to block all of its attendant ills.

Dancho: Microsoft's Digital Crimes Unit has been getting a lot of press attention lately, thanks to their Rustock and ZeuS take down campaigns. However, what the mainstream media is missing is the fact that Microsoft is basically shutting down U.S hosted crimeware infrastructure, a drop in the bucket when it comes to active malware/crimeware campaigns. In the age of fast-fluxed command and control servers, do you believe Microsoft's efforts have a short-lived, short-term oriented result in response to the threat posed by malicious software? Why and why not?

Brian: I think we can continue to expect to see Microsoft doing whatever it can to disrupt cyber criminal activity, because 95 percent of it or more is aimed squarely at their customer base. Whether the gains from those take downs and targeted actions have long or short-term consequences may not be so important to Microsoft. From my lengthy interviews with Microsoft's chief legal strategist on this subject, it was clear that their first order of business with these

actions is raising the costs of doing business for the bad guys, and I think on that front they probably will succeed in the long run if they keep going after them as they are.

Dancho: On a periodic basis, you and I often receive the attention of cybercriminals who leave messages embedded in the source code of malicious page, an actual file name, or within the source code of a particular piece of malware in general.

In 2011, F-Secure intercepted a trojan where the authors left a "[DANCHODANCHEV AND BRIANKREBS GOT MARRIED](#) " mutex. What was your initial reaction when you saw this? After all these 'touch points' left by the cybercriminals, does this mean that your work is actually making an impact within the cybercrime ecosystem, and is logically getting noticed by sophisticated cybercriminals, or do you believe it basically kids looking for public attention?

Brian: I consider it a badge of honor that these guys bother to thumb their noses at me. The most recent one I'm aware of was whoever was in charge of coding the Citadel Trojan added some strings in the malware that said, ""Coded by BRIAN KREBS for personal use only. I love my job & wife". Sort of a friendly jab and a vague, nonspecific threat rolled into one. Sometimes it is just kids looking for attention, but by and large I think most of these guys truly resent having any outside light -- especially from "amers" or Americans -- shed on their operations. They also don't like it when you distill their operations, norms or processes into bite sized chunks that demystify their ecosystem or forums.

Dancho: As a compliment to your research, your blog is often subjected to DDoS (denial of service attacks) attacks. How often do you get them, and do you have your ISP's full support in mitigating them? Are you also aware who's attacking you based on the data gathered in the log files? What tools are they using?

Brian: As I write this, my site is under attack, and has been for roughly two weeks straight now. My ISP has been fully supportive in helping me out. I'd rather not comment on the frequency, but sometimes I am aware who the cowards are. For instance, last year

some [rogue pharmaceutical spam gangs took out my site with the help of servers at Microsoft](#), and then proceeded to register tens of thousands of porn and pill domains in my name with stolen card data.

I've also suffered [DDoS attacks at the hands of Russkill](#), which is a popular DDoS bot kit.

Late last year, my inbox was bombed with 100,000+ emails using a commercial fraud tool that is typically leveraged against cyberheist victims as a way to obscure an email alert or authorization from the target's bank.

Go through previous Q&As of the Week:

[Q&A of the Week - 'The current state of the crimeware threat' featuring Thorsten Holz](#) [Q&A of the Week: 'The current state of the cyber warfare threat' featuring Jeffrey Carr](#) [Q&A of the Week: 'The current state of the cybercrime ecosystem' featuring Mikko Hypponen](#)

Dancho: Occasionally, the security community in combination with law enforcement, shuts down a widely popular underground community, or releases the results of a successful sting operation, proving that they have infiltrated this community. Do you think that cybercriminals act in a different way when they know that they're being watched? Do you believe that a researcher's or a LE agent's involvement in underground market trade for the sake of preserving access to this community is worth it? What is the best way to handle these communities? Infiltrate them, passively observe them, or shut them down as soon as you come across them?

Brian: I can't speak for law enforcement activity, but as a journalist and investigative reporter, I'm always sad to see these communities go away. I think it's safe to say that most of them are already infiltrated by several national law enforcement organizations. I'd be very surprised if they were not. Some operating right now probably were even set up by law enforcement. We've seen them do that a few times before. I think most of the fraudsters who've been doing this long enough probably understand that and act accordingly. Others do not, and that is why you tend to see lots of people come

and go, but the same core group of a few hundred guys are the top dogs on most important forums.

Communities and crime forums are great places to learn intelligence about upcoming and ongoing attacks, breaches, 0days, etc. Shutting them down seems to me to be counterproductive, since you almost always force the forums to go more underground and use more security features to keep untrusted people out, and known sources of intelligence go away, or worse yet change their nicks and contact info and all of a sudden a source you have developed you may never see or hear from again.

Dancho: Risk-forwarding has been an inseparable part of the cybercrime ecosystem for years. From [malware-infected hosts as stepping stones](#) , to the one of the most prolific problems in recent years - [the rise of money mule recruitment](#) . Based on personal research, I'm currently aware of a single -- market leader -- vendor offering web site templates and full documentation for potential money mule recruiters. Are you also observing the standardization of the recruitment process thanks to a single vendor offering the advertising creative, or are you currently observing multiple vendors of web site templates and full documentation?

Brian: I've identified quite a few distinct money mule recruitment networks. I don't know about templates, but many of them tend to recycle the same HTML content and change the names of the fake companies. That's handy I guess for keeping track of which group recruited which mules, but beyond that I'm not sure it tells you much. What I have noticed is that money mules are the bottleneck for this type of fraud, and often times the cyber crooks will leave money in the victim's account because they simply didn't have enough mules to help them haul all of the loot. So with any one victim, it's typical to find mules recruited through 4-6 different mule recruitment gangs, because the fraudsters who outsource this recruitment will simply go from one to the other purchasing the services of these recruitment gangs until they've got enough to help them haul the loot, or they've exhausted the available mule supply. But usually, the mule gangs don't have any problem finding new recruits.

Dancho: Are [reshipping mules](#) more popular than [money mules](#) in general, or it depends on the recruiting organization's objectives?

Brian: I think reshipping mules tend to be more useful. Most regular money mules are one-and-done. They're used for a single task and then discarded (although one group I am following re-uses money mules as many times as they can before the mule starts to ask for their monthly salary). Typically, a reshipping gang will get 3-5 packages reshipped per weekday per mule, and the average reshipping mule works for 30 days before figuring out they've been working for free and great personal risk and they're never going to get paid, or the check they got from their employer just bounced. But several mule gangs I'm aware of do both reshipping and money mules interchangeably.

Dancho: The Dutch Rabobank is rumored to be blocking access to its debit cards outside the EU in order to prevent successful ATM skimming attacks. Are you aware of a practice called "Credit Card Tourism" where dozens of people with multiple plastics take buses and travel across Europe, taking money out of ATMs on the road?

Brian: No, but it sounds like a nice way to see Europe, if you can avoid the slammer along the way. :)

Dancho: Do you believe gullible money mules should hold no responsibility for their actions, or do you believe they are basically aware of the fraudulent nature of the job proposition, even before the start? Do you think policy makers are on the right track when it comes to addressing the money mule recruitment problem internationally? Why and why not?

Brian: I think about half are just not the sharpest crayons in the box. Many of them will request benefits and mileage reimbursement, and some will believe they're even getting promised insurance benefits. The other 50 percent probably know or suspect it's fraud but aren't asking too many questions because they're out of a job or a single parent (or quite often both) and they need to make their rent. Do I think they should be held accountable? Absolutely. I see no difference between this activity and writing bad checks, which people

get put in jail for all the time. Will a prosecutor be able to understand the crime and explain it well enough to a jury of the mule's peers -- many of whom aren't smart enough to figure out how to get out of jury duty in the first place -- that THEY wouldn't have fallen for a similar scheme -- that he can get a conviction? That's another question entirely.

Dancho: [DDoS for hire](#) vs [DDoS extortion](#) - Which of these underground market segments is more popular these days, based on your own personal observations?

Brian: No idea, sorry.

Dancho: With [Facebook's rumored interest in online gambling](#) do you think it will successfully position itself as a target for DDoS extortionists once the platform scales enough and starts attracting huge portions of U.S based Facebook users? Or will cybercriminals continue targeting lower profile sites in an attempt to avoid attracting the attention of law enforcement?

Brian: I'm almost certain that Facebook get attacked constantly, but you should probably ask them. I don't know much about any ambitions they may or may not have in the gambling space, sorry.

Dancho: Do you believe in the concept of cyber fraud insurance? Should a bank that fails to protect it customer's assets be held responsible for the fraudulent transactions that took place, or is it ultimately the responsibility of the customer to ensure that he's E-banking in a secure fashion?

Brian: I think it's a nice idea, but it merely glosses over the underlying problem. Cyber insurance is basically a way of shifting the risk, but doing so in a way that may not be where the cost for assuming that risk ought to reside. What's easier and makes more sense: A bank spending a few million dollars more and really thinking about and implementing adaptive security, or doing the bare minimum and having all of their customers have to either buy insurance or take extreme measures to protect themselves when banking online? The latter is the situation we have today, for better or for worse.

Dancho: There's been a lot of buzz recently, surrounding advanced persistent threats (APT attacks). Do you differentiate between targeted attacks and APTs, or from a marketing perspective, the buzz was basically re-branding of a well known process in order to reboot its public awareness life cycle?

Brian: I think if there has been a net positive about the shift in focus (at least from the mainstream security industry) away from traditional threats to APT attacks it is in the increased attention paid to social engineering attacks, which form the basis of most successful attacks today. Oday threats get a lot of press and are frequently associated with APT attacks, but it is far more common for these attacks to leverage known vulnerabilities for which there are patches, much like exploit packs that are used in many Zeus attacks and other more traditional cyber crimes. Unfortunately, educating users about what not to click on or trust or open is always an uphill battle. There are some things that companies could be doing more on this front, and I'd like to see more firms randomly test their employees to help speed the process of learning how not to fall for phishing and social engineering scams.

Dancho: Despite the numerous shut downs of payment processing gateways working with the scareware industry, scareware remains one of the most profitable monetization strategies within the cybercrime ecosystem? Do you agree or disagree, why and why not? Also, do you believe that the scareware business model can be best undermined for targeting the payment gateways, or perhaps you may have something else on your mind?

Brian: I don't think scareware is the same scourge it used to be, although it's clearly still a problem. I would say this problem -- like the pharma spam problem -- must be attacked at the payment processing point; that is where it makes the most sense. There are some things afoot in the payment processing space that I think will probably start to show major results in the coming months on this front, but the proof will be when the scareware partnerka programs start dying off completely because the business model has dried up. I think we can expect to see the costs of acquiring banks taking on

this business continue to rise, and that will help make the scareware industry less profitable and less attractive for scammers.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns | ZDNet

With just four days until the [FIFA World Cup](#) begins, cybercriminals have already started showing their interest in taking advantage of the event, by launching [targeted malicious PDFs/malware serving campaigns](#), blackhat SEO and fraudulent propositions, followed by lottery winning notifications/letters of claim themed scams.

Considering that, these threats and exploitation tactics are prone to intensify throughout the entire event, let's review some of the most commonly used attack vectors, and discuss the risk mitigation strategies for each and every one of them.

The threats and the fraudulent schemes

The following list doesn't aim to achieve conclusiveness, instead it would discuss the most prevalent threats based on the historical "performance" of malicious attackers, and scammers in general.

[Targeted malware attacks serving client-side exploits](#) - The combination of a recently announced [zero day flaw affecting Adobe's most popular products](#), and the global proportions of the FIFA World Cup, clearly offer a malicious attacker the opportunity to capitalize on the event. According to Symantec, based on the campaigns analyzed since April, malicious PDFs continue representing the highest percentage of malicious attachments - *.pdf 41%.exe 18%.doc 14%.xls 7%.scr 4%.ppt 1%*. Their findings confirm [the findings from a related report](#), indicating that outdated Adobe flaws for which patches are available, represented 80% of all exploits for 2009. What's driving the success of these malicious campaigns? With or without the recent Adobe zero day, the malicious attackers have realized that just because a patch is available, it doesn't necessarily mean that hundreds of thousands of Internet users are patching themselves. And they should.

[419/Lottery Scams](#) - According to the [2009's IC3 Internet Crime Report](#), advance fee fraud represented 9.8% of all complaints. The

percentage is naturally much higher due to the unknown number of people that didn't report the fraud. Largely underestimated as a serious threat, lottery scams usually cost a small fortune to the affected victim. And due to their targeted nature -- the majority are sent manually and usually originate from Africa based IPs -- the scammers often succeed in tricking the gullible user. Once the user, now victim, is hooked, the "*Winning Notification* " slowly transforms into a advance fee based fraud, where in order to obtain the millions that you never really won, you would need to send back a decent amount of money. Don't.

Blackhat SEO (Search Engine Optimization) campaigns serving scareware - Blackhat SEO, involves the process of on purposely hijacking trending buzz story across the web, in order to capitalize on the hijacked traffic by serving client-side exploits, or most commonly scareware. There's a common misunderstanding regarding blackhat SEO campaigns these days, with a large number of users thinking that a cybercriminal is manually monitoring these trending topics in order to hijack them. Which is not true, since the process is semi-automatic, in fact on the majority of occasions they aren't even aware that they're targeting a particular topic.

Spamvertised fraudulent offers, phishing attempts - According to the 2009's IC3 Internet Crime Report, non-delivery of merchandise and/or payment represented 11.9% of all the complaints. Moreover, the scammers are also well known for keeping track of different promotions, which they can easily brandjack and attempt to obtain sensitive data from the affected users. One of these examples is **Visa's "Go Fans" campaign** - "*Phishing samples spammers are targeting the Visa brand, which is one of the six global FIFA partners. Visa announced a "Go Fans" promotion offer in which card holders get the chance to win a trip to South Africa to experience the 2010 World Cup matches. Aware of the fan frenzy involved with watching live World Cup games, phishers are in the right (albeit criminal) business of trying to make money out of it.* "

Sample FIFA World Cup 2010 themed Lottery Scam:

Sample targeted campaign, using malicious Excel files:

Risk mitigation strategies

Targeted malware attacks serving client-side exploits - With malicious PDFs representing such a high percentage of the exploits used, perhaps an [alternative PDF reader such as the Foxit Reader](#), is worth considering. As well as: taking care of [outdated third-party applications](#) in combination with NoScript and [least privilege accounts](#), or complete [sandboxing](#)/[isolated web browsing](#), in order to ensure that what happens in the sandbox, stays in the sandbox.

419/Lottery Scams - Although the professional layout of these messages is improving, perhaps the single most important mitigation strategy, one that no software vendor can provide you with, is the lack of gullibility when someone tells you that you've just won 1 million dollars. [Don't be naive](#), and once you spot the scam, [consider reporting it](#).

Blackhat SEO (Search Engine Optimization) campaigns serving scareware - The protection tips for mitigating client-side exploits serving campaigns, fully apply to the scareware threat. For additional information on what exactly scareware/rogue security software is, and how to protect from it, consider going through the "[The ultimate guide to scareware protection](#)".

Spamvertised fraudulent offers, phishing attempts - despite the fact that [millions of people admit they click and interact with spam/phishing emails](#), these emails are not longer 100% fraud oriented, but often as the first touch point for a targeted client-side exploits serving campaign. Therefore, avoiding any interaction with them, next to reporting them as spam, is highly recommended.

Proof of Concept "carpet bombing" exploit released in the wild | ZDNet

In what appears to be an attempt to provoke Apple to reconsider its currently passive position on the severity of the dubbed as "carpet bomb"

flaw, a working Proof of Concept exploit code has [been released](#) at Liu Die Yu's security blog :

[Nitesh Dhanjani](#) discovered [that](#) Safari for Windows puts downloads automatically to Desktop and argued this can potentially make a mess of Desktop, naming it the effect of "Safari Carpet Bomb". Later Microsoft issued an [advisory](#) stating "remote code execution on all supported versions of Windows XP and Windows Vista" and "Aviv Raff for working with us and reporting the blended threat of Safari and Microsoft Internet Explorer". Aviv Raff [posted on his blog](#) "Safari pwns Internet Explorer", clarifying "this combined attack also exploits an old vulnerability in Internet Explorer that I've already reported to them a long long time ago".

The old vulnerability that Aviv Raff reported to Microsoft long time ago is described in two articles by Aviv Raff: [IE7 DLL-load hijacking Code Execution Exploit PoC](#) , and [Internet Explorer 7 - Still Spyware Writers Heaven](#) , both dating back to 2006(yeah that's really "a long long time ago"). This vulnerability lies in Windows Internet Explorer loading program library files(DLL) from user's Desktop instead of its own library file folder(usually C:\WINDOWS\SYSTEM32), when filenames are set to some specific values.

Liu's posts also mention [a new security threat in Safari for Windows](#) , different than the "blended threat" described by Microsoft, and summarizes [the whole fiasco](#) about who's responsible for what in short :

Safari for Windows puts downloads to Desktop by default without a dialog box(such as the "File Download" dialog box in IE). Well, this is in fact a quite reasonable and convenient feature - downloading and saving requested file to user's Desktop by default. This feature

itself does not constitute a mistake. What really makes the "blended threat" is some problem in loading program library files(DLL) by Windows Internet Explorer(and probably others)

In a situation where [researchers](#) and [anti-malware groups](#) clearly demonstrate the possibility for abuse of this vulnerability, Apple's passive attitude taking into consideration the possible impact on the stereotype of their software's invincibility courtesy of their PR folks, can only be changed by [going full disclosure](#) with the exploit, no matter how much [vendors hate it](#) . Nothing's impossible, the impossible just takes a little longer, and so is finding bugs in software pitched as the most secure one.

How to protect yourself? Watch what you click on, change the default download location of the browser, or consider avoiding Safari for Windows until the flaw gets some attention at the first place, and hopefully gets fixed later on.

Pro-Serbian hacktivists attacking Albanian web sites | ZDNet

The rise of [pro-Kosovo web site defacement groups](#) was marked in April, 2008, with a massive web site defacement spreading pro-Kosovo propaganda. The ongoing monitoring of pro-Kosovo hacking groups indicates an ongoing cyberwar between pro-Serbian supporting hacktivists successfully defacing Albanian sites, and building up capabilities by releasing a list of vulnerable Albanian sites (remote SQL injections for remote file inclusion, defacements or [installing web shells/backdoors](#)) to assist supporters into importing the list within their [do-it-yourself web site defacement tools](#) .

According to Serbian hacking groups, independent Albanian web site defacers initially started attacking their sites later on joined by Kosovo Hacking group. In response, Serbian hacking groups have started distributing a segmented list of remotely exploitable Albanian sites and encouraging others to join the initiative and attempt to deface the sites. For the time being, Partia Demokracia Sociale (**Social Democracy Party of Albania**), AlbiInvest (**The First Investment Forum Albania-United Kingdom**), and **Tirana Bank** are among the high-profile sites that have been defaced next to many others.

This incident greatly represents the capability building process and the degree of information sharing between Serbian groups empowering everyone with an already verified hit list of vulnerable Albanian sites.

Both groups are currently in a ceasefire phrase, trying to figure out who provoked who, by requesting group members to participate in the ongoing discussing. However, the possibility to engineer hacktivism tensions remains just as realistic, as engineering cyber warfare tensions is, by making it look like that the source of the attack is coming from a party what would be attacked based on the lack of evidence verification - in this minor cyber conflict the groups are in fact talking with each other. Moreover, in the long-term, [web](#)

[site defacement groups](#) realizing the market value of their know-how, will inevitably start contributing with spammers, phishers and malware authors in a much broader sense than the current degree of collaboration - [selling acccess to compromised web servers only](#) .

Privacy flaw exposes Paris Hilton and Lindsay Lohan's private MySpace photos | ZDNet

The recently introduced [data availability initiative](#) at MySpace allowing everyone to share their profile data with other

community and social networking sites across the Web, has just suffered its first major privacy flaw [exposing the private photos of Paris Hilton and Lindsay Lohan](#), prompting Yahoo and MySpace to [disable the data availability](#) between the services [until they fix the flaw](#):

Pictures of Paris Hilton and Lindsay Lohan from private MySpace profiles can be seen by anyone on the Internet, thanks to a flaw in a system that helps the social-networking site share information with other Web sites. The incident underscores a new challenge for businesses: Security becomes a multi-front challenge once you start sharing information outside your walls.

Byron Ng — a computer technician who earlier this year found a way to access Paris Hilton's Facebook page — walked the tech-gossip blog Valleywag through a 15-step process that allows people to see supposedly-private pictures and other information by first logging into Yahoo, which is one of the sites that shares information with MySpace.

With Paris Hilton's T-Mobile Sidekick account hacked two years ago ([Hilton's mailbox](#); [Hilton's contact list](#); [Hilton's photos](#)), followed by her private Facebook private photos exposed last month, it's becoming a rather common event to demonstrate a major privacy exposing leak or a security flaw by testing it on celebrities with the idea to attract as much attention as possible. All of these hacks wouldn't be possible if their "privacy through obscurity" MySpace profiles weren't a public secret. For instance Paris Hilton's private profile (myspace.com/cherubrawk) and Lindsay Lohan's profile (myspace.com/privacycunt) have already been tracked down by

fans, therefore positioning them on the top of the target list for testing of flaws.

From another perspective, celebrity hacking is a win-win-win situation for both the celebrities enjoying some publicity, the vulnerable services that would provide a live fix for the millions of their users, and [the celebrity hacker](#) for, well, being the celebrity hacker. It's also a great way to demonstrate how one service is undermining the already set privacy preferences by another service, as in this case you have an integration flaw at Yahoo undermining the privacy preferences set on a MySpace profile.

Popular free antivirus apps for Android fail anti-malware tests | ZDNet

Is free always better than paid, in respect to antivirus software, or does it basically [offer a false feeling of security?](#)

The [latest comparative review of free antivirus applications for Android](#), courtesy of AV-Test.org, offers an interesting insight into just how effective or ineffective those applications really are.

The researchers tested the following free antivirus applications against 10 widely spread malicious apps.

Antivirus Free
BluePoint Antivirus Free
GuardX Antivirus
Kinetoo Malware Scan
LabMSF Antivirus beta
Privateer Lite
Zoner AntiVirus Free

and two commercial antivirus apps offered by F-Secure Mobile Security and Kaspersky Mobile Security.

The findings?

The scanned test set contained 83 Android installation packages (APK) and 89 Dalvik binaries (DEX). No files were older than 5 months. **The best results claimed the products of Kaspersky and F-Secure, which detected at least 50% of all malware samples already in inactive state. The best free app was Zoner AntiVirus Free with 32% detected malicious apps.** All other scanners detected at best 10% of the apps, some didn't detect anything at all.

BluePoint AntiVirus Free, Kinetoo Malware Scan and Privateer Lite still warned against one malicious app. Antivirus Free by Creative Apps, GuardX Antivirus and LabMSF Antivirus beta failed completely.

Was the test a complete overview of the market for free Android-based antivirus applications? Not at least according to [MSNBC](#) since

it failed to include the following applications in the test - AVG Antivirus Free, BitDefender Mobile Security, Lookout Mobile Security, and Norton Mobile Security.

What do you think? Does free antivirus software offer a false feeling of security?

Talkback.

Popular brands impersonated in latest malware campaign | ZDNet

Multiple vendors are [reporting on a](#) currently ongoing [scareware and client-side exploits serving](#), spam campaign, brand-jacking Best Buy, Chase, Macy's, Target.com and Evite.

The payments-themed campaign is enticing users into clicking on on a malicious link which attempts to exploit client-side vulnerabilities targeting [Java, Acrobat Reader etc](#). in between loading a [scareware-serving](#) page ([antivirus_24.exe](#)), tricking users into thinking they're [infected with malware](#).

Sample subjects include:

"Thank you for scheduling your online payment"

"Thank you for your payment"

"Thanks for planning your event with Evite"

"Your Target.com order has been shipped"

"Thank You, Your Anti-Virus Protection Plan has been renewed"

This campaign is directly related to last month's "[Malware Watch: Malicious Amazon themed emails in the wild](#)" campaign, as well as to the [Xerox WorkCentre Pro scanned document themed campaign](#), with both campaigns managed by the same cybercriminals.

Windows users are advised to keep their [3rd party applications](#) and browser [plugins](#) up-to-date, use [least privilege accounts](#), securely [handle active content](#), or [completely](#) isolate their [Internet activities](#), in order to mitigate a huge percentage of the risk posed by such attacks.

Image courtesy of WebSense.

Police arrest Mariposa botnet masters, 12M+ hosts compromised | ZDNet

According to a [statement published by the Spanish Ministry of Interior](#) , the botnet masters behind a 12M+ infected hosts [botnet dubbed Mariposa](#) , were arrested in a cooperative effort between law enforcement, security vendors and the academic community.

Following the arrest of one of the botnet masters, law enforcement officers seized sensitive data belonging to 800,000 users across 190 countries, and found [evidence of infected hosts](#) located within the networks of [500 of the US Fortune 1,000 companies and more than 40 major banks](#) .

Just how sophisticated were the botnet masters behind Mariposa? You'll be surprised to find out.

On December 23 2009, in a joint international operation, the [Mariposa Working Group](#) was able to take control of Mariposa. The gang's leader, alias Netkairo, seemingly rattled, tried at all costs to regain control of the botnet. **As I mentioned before, to connect to the Mariposa C&C servers the criminals used anonymous VPN services to cover their tracks, but on one occasion, when trying to gain control of the botnet, Netkairo made a fatal error: he connected directly from his home computer instead of using the VPN.** Netkairo finally regained control of Mariposa and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.

The initial reports describe the group as not so technically sophisticated "normal people" making a lot of money through cybercrime. A logical question emerges - how is it possible that a group of "normal people" can build such a massive botnet? By outsourcing.

Go through related posts: [Malware Infected Hosts as Stepping Stones](#) ; [The Cost of Anonymizing a Cybercriminal's Internet](#)

[Activities](#) ; [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two](#) ; [Zeus Crimeware as a Service Going Mainstream](#) ; [Managed Polymorphic Script Obfuscation Services](#)

The name [Mariposa actually means butterfly](#) , which is the original name of a commercially distributed DIY malware kit, sold online for 800/1000 EUR, unless of course the arrested botnet masters weren't using a pirated version, which is ironically, a common practice within the cybercrime ecosystem these days. What's particularly interesting about the malware was the fact that it was using its own UDP-based protocol for communication, which according to the original author was developed with stealthiness in mind since UDP connections are rarely logged.

Moreover, the bot has typical for modern malware releases anti-debugging features, as well as built-in DDoS functionality relying on TCP and UDP flood tactics. The three main propagation vectors include MSN, removable media, and through P2P, targeting the following networks - *Ares, Bearshare, Imesh, Shareaza, Kazaa, Dcplusplus, Emule, Emuleplus, Limewire* .

Just like the majority of commercial DIY malware releases, this one also includes a disclaimer attempting to position it as a "tool for educational purposes only", with the DDoS option itself described as a tool for "stress testing" your own infrastructure. Also, despite the initial claims that the "[mastermind of 'botnet' scam remains a mystery](#)", commercial releases by the original coder of the bot have been circulating in the underground marketplace since 2007. With the recent bust of his customers, he'll be definitely keeping a low profile for a while.

The Mariposa botnet is the tip of iceberg in respect to DIY botnets ([Research: Small DIY botnets prevalent in enterprise networks](#) ; [Inside the botnets that never make the news - A Gallery](#)) aggregated using commercially, or freely available malware kits.

What this incident proves is that not only is cybercrime becoming easier to outsource in 2010, but also, that even inexperienced people can quickly gain access to capabilities once reserved for sophisticated attackers.

Google

disruptive.individuals@gmail.com

Multiple Url Opener – Free One-Click Tool, No Install Required

If the URLs do not open, it means the pop-ups are blocked in your browser.

Below are the instructions on how to disable pop-up blockers.

Chrome

- Click on the icon that appears in address bar

- Select “Always allow pop-ups from

<https://www.websiteplanet.com/>

Firefox

- Open Settings

- Open Content Tab

- Under Pop Ups Click Exceptions

- Enter <https://www.websiteplanet.com/> and select Allow

- Save and Restart Firefox

Edge

- Open Settings

- Go to Advanced Settings

- Switch Block Pop Ups Off

- After using URL Opener Roll back these settings

CLOSE

Spamvertised Post Office Express Mail (USPS) emails lead to malware | ZDNet

A currently spamvertised malware campaign is brand-jacking the USPS in an attempt to trick users into downloading and executing a malicious file.

Sample subject: Post Express Information. Your package is available for pick up. NR[random number]

Sample attachment: [Post_Express_Label_ID_\[random number\].zip](#); [Post_Express_Label.exe](#)

Sample message: *Dear client Email notice number.[random number]. Your package has been returned to the Post Express office. The reason of the return is "Error in the delivery address" Important message! Attached to the letter mailing label contains the details of the package delivery. You have to print mailing label, and come in the Post Express office in order to receive the packages! Thank you for using our services. Post Express Support.*

Users are advised to avoid interacting with suspicious file attachments.

Spamvertised 'PayPal payment notifications' lead to client-side exploits and malware | ZDNet

PayPal users, beware! A currently [spamvertised malicious campaign](#) is impersonating PayPal in an attempt to trick end and corporate users into clicking on [exploits-serving links](#) found in the emails.

Upon clicking on the links, users are exposed to the client-side exploits served by the most popular Web malware exploitation kit currently in use by cybercriminals - the [BlackHole exploit kit](#).

The campaign ultimately drops the following [MD5: 4f58895af2b8f89bd90092f08fcbd54f](#) currently detected by 17 out of 42 antivirus vendors.

Who's behind this campaign? Over the past couple of months, a single cybercriminal, or a gang of cybercriminals have been systematically rotating the impersonation of multiple companies in an attempt to trick end users into clicking on their exploits-serving links.

So far, the gang has impersonated [U.S Airways](#), [Verizon Wireless](#) and [LinkedIn](#), and the campaigns show no signs of slowing down.

End and corporate users are advised to ensure that they're running the [latest versions of their third-party software](#), and [browser plugins](#) in an attempt to avoid being exploited by the BlackHole web malware exploitation kit.

Spamvertised FedEx notifications lead to malware | ZDNet

A currently ongoing spamvertised campaign is [brand-jacking FedEx for malware-serving purposes](#).

Sample attachments: FedEx letter.zip; FedEx letter.exe **Sample subject:** FedEx notification #random number **Sample message:** *Dear customer. The parcel was sent your home address. And it will arrive within 7 business day. More information and the tracking number are attached in document below. Thank you. © FedEx 1995-2011*

Upon downloading the executing the attachment, the malware attempts to download two additional binaries, next to sniffing for FTP credentials off infected hosts.

Detection rate for [FedEx letter.exe](#).

Spamvertised 'Facebook. Your password has been changed!' emails lead to malware | ZDNet

Malicious attackers are [currently spamvertising malicious attachments](#) impersonating [Facebook's Support Team](#). Upon execution the sample Mal/Zbot-AV drops additional malware.

Sample subjects: *"Facebook. Your password has been changed! [NUMBER]" "Facebook. The new password to your account. [NUMBER]" "Facebook Support. Personal data has been changed! [NUMBER]"*

Sample message: *Dear user of FaceBook. Your password is not safe! To secure your account the password has been changed automatically. Attached document contains a new password to your account and detailed information about new security measures.*

Thank you for attention, Administration of Facebook.

Users are advised to avoid interacting with suspicious attachments.

See also:

[Spamvertised "Regeest Rejected" campaign leads to scareware](#)
[Spamvertised Post Office Express Mail \(USPS\) emails lead to malware](#)
[Spamvertised DHL notifications lead to malware](#)

Spamvertised 'Facebook notification' leads to exploits and malware | ZDNet

Security researchers from M86 Security Labs, have intercepted a [spamvertised malware campaign](#) using bogus Facebook notifications as a social engineering element.

Spamvertised through the Cutwail botnet, the malware campaign is impersonating Facebook in an attempt to trick users into clicking on a bogus Facebook notification message. However, the HTML source of the email reveals a link to a malicious iFrame leading to the BlackHole web malware exploitation kit. Upon clicking on the link, the exploit kit will check for remotely exploitable client-side applications and browser plugins, and serve the malware.

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Spamvertised Easter Greetings lead to malware | ZDNet

Security researchers from McAfee Labs are reporting on a currently ongoing [event-based social engineering attack](#), aiming to trick users into clicking on a link found in a malicious email.

The spamvertised emails come using "*Easter Greeting from Alex*" subjects, and are using an animated image including a "*Download Animated Greeting Here*" body. Upon clicking on the link, the user is exposed to a password-stealing malware variant of PWS-ZBot.

With Easter only a few days away, cybercriminals are quickly adapting to the event-based social engineering potential presented by the holiday.

Users are advised to [avoid interacting with suspicious links and email attachments](#) found in email messages.

Spamvertised 'DHL Tracking Notification' emails serve malware | ZDNet

Security researchers from Sophos have intercepted a currently circulating malware campaign that's using ['DHL Tracking Notification' themed emails in order to serve malware](#).

The emails contain a ZIP attachment -- *DHL-Express-Delivery-Notification-Details_03-2012_[random string].zip* -- that's containing the actual malicious code. The malware is currently detected as Mal/BredoZp-B and Mal/Zbot-FV.

This isn't the first time that cybercriminals are impersonating DHL. In the past, [they have also](#) impersonated [UPS](#) and [FedEx](#), once again in an attempt to trick end and corporate users into downloading and executing a malicious attachment.

End and corporate users are advised to avoid interacting with the emails, and to report them as spam/fraudulent immediately.

Spamvertised DHL notifications lead to malware | ZDNet

A currently [ongoing malware campaign](#) is brand-jacking DHL for [malware-serving purposes](#). The spamvertised emails arrive as DHL Notification using DHL_tracking.zip; doc.zip; document.zip file names.

Sample message: *Dear customer! The parcel was send your home address. And it will arrice within 7 bussness day. More information and the tracking number are attached in document below. Thank you. 2011 DHL International GmbH. All rights reserved.*

Upon execution the SpyEye crimeware campaign phones back to multiple URLs aiming to obtain additional modules for sniffing FTP credentials off malware-infected hosts.

Detection rates for the malware; [DHL_notification.exe](#); [doc.exe](#); [DHL_tracking.exe](#)

Spamvertised 'Cancellation of the package delivery' emails serving malware | ZDNet

Security researchers from Sophos have intercepted a [currently spamvertised malware campaign](#), impersonating the Royal Mail office.

Spamvertised subjects include:

Error in the delivery address No30173
You should come to the Royal Mail office and receive a package
Track your shipment No24127
Cancellation of the package delivery
Track your parcel No9782
A package is available for reception
Get your parcel No083
Error in the delivery address No40046009
Error in the delivery address No0633376
Delivery Problem
Royal Mail Delivery information

Spamvertised message:

Dear customer.A courier did not deliver the package to your address.Reason: The package is too largeInformation about your package is attached to the letter.Read all information carefully and come to the "Royal Mail" office to receive your package.Thank you for your attention.Royal Mail Service.

In this campaign, cybercriminals are enticing end users into downloading and execution a malicious .ZIP attachment currently detected as Mal/BredoZp-B and Mal/EnckPK-AAT (MD5: 6bd53a62c768f7ce8663310ed404b89c).

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Spamvertised bank statements serving scareware | ZDNet

Security researchers from BitDefender are reporting on a [currently spreading malware campaign](#) using bogus bank statements as a social engineering element of the campaign.

The spamvertised executables **Financial_Statement.exe** ; **Postal_document.exe** drop additional files when executed, namely the [rogue antivirus software also known as scareware](#).

Users are advised to be extra caution when dealing with executable email attachments, and and report them as spam as soon as possible.

Spamming vendor launches managed spamming service | ZDNet

A spamming vendor known as the SET-X Corporation, has recently launched the distributed SET-X Mail System, a sophisticated managed spamming service available for rent on a monthly basis starting from \$2000, promising to achieve "spamming speed" of 5000 to 7000 emails per minute and over 1 million spam messages per day, courtesy of the 5000 bots it comes preloaded with.

Let's analyze the spamming service, what makes it tick, and discuss some of the emerging trends related to the overall outsourcing of each and every segment of cybercrime.

The market segment for [managed spamming services](#) is still in its introduction stage, with several unique providers of [such](#)

[managed services](#) whose do-it-yourself systems and zero complexity mentality are poised to empower many new entrants into the spamming business. The SET-X Mail System in particular, is a typical example of a "one stop spamming shop", which compared to legitimate companies that are able to occupy and serve all the market segments related to their particular product or a service through M&A (mergers and acquisitions) with different companies, has managed to vertically integrate on their own and logically provide anything a spammer could possibly need from a spamming service such as :

- dedicated staff of four people updating the malware binaries and reachable 24/7

- daily introduction of new malware infected hosts

- the ability to purchase recently harvested email databases for a particular country in order to use them in localized spam campaigns, with the translation service for the messages provided by the same vendor

- the option to purchase an unlimited number of [automatically registered email accounts](#) at popular web based email providers in order to integrate them within the ["unique legitimate senders"](#)

spamming method

unlimited support of spam templates also known as macroses

unlimited number of email databases to integrate and use simultaneously

low total cost of ownership (TCO) and 99% uptime of the command and control server due to the fact that the malware infected hosts obtain commands dynamically from secondary servers in order to ensure that they never expose the central one

Speaking of [vertical integration](#) , SET-X Corporation's current inventory of harvested email addresses available for sale to customers of its spamming service seems to have been anticipated as a possible revenue source, aiming to further develop the business relationship with the current customers. Their current inventory :

"Russia (private citizens) - 16 000 000 emails Ukraine (commercial) - 3 300 000 emails U.S.A (private citizens) - 118 000 000 emails Western Europe (private citizens) - 13 000 000 emails Europe (private citizens) - 46 000 000 emails"

How sophisticated is in fact the service? SET-X Corporation has extensively described the spamming service in their marketing pitch, translated from Russian to English as follows :

"- Flexible and convenient Web based interface, detailed statistics while sending, changing any settings (mail databases, texts, macros)

- User-friendly web based interface - start spamming from day one

- Automatic "spamming capabilities" assessments of the bot allowing you to think about your business and not about the technical details behind it

- Daily malware updates, four programmers allocated for every server, sending automatic ICQ notifications whenever the malware gets updated

- Automatic optimization of the spam campaign by first allocating the bots with clean IP reputation

- Optional is the option to chose whether or not a dedicated "spamming engineer" should be allocated to your server

- His responsibilities include introducing a higher number of bots if requested, ensuring that dead bots get disconnected from your server, and providing personal advice on optimizing your campaigns and bypassing anti-spam filtering through the built-in multi RBL checking feature

A brief description of the system:

1. The system is automatically harvesting the outgoing and incoming email addresses on the infected hosts and the associated accounting data, supporting the following clients : - Mozilla Thunderbird - Outlook Express - MS Outlook - The Bat - Opera

2 . The bot automatically defines its MX and PTR records, if they are present it switches to Direct SMTP mailing which means that it can send the spam directly to the recipients using the MX and PTR DNS records of the bot, enforcing direct sending even without MX and PTR records is also possible

3. The bot automatically defines its MX and PTR records, if they are present it switches to Direct SMTP mailing which means that it can send the spam directly to the recipients using the MX and PTR DNS records of the bot, enforcing direct sending even without MX and PTR records is also possible

4. The central control server automatically assigns different regional servers to the bots, and rotates them periodically for security purposes

5. All the information about the spam campaigns and the bots can be exported and syndicated with another regional server as requested, with the regional server dynamically establishing links with other regional servers so that it never really knows the address of the central command server

6. There are several different ways of sending spam using this service :

1) Direct spamming from the legitimate email accounts of the infected computers, with the system automatically syndicating all the available legitimate emails whose accounting data naturally stolen due to the malware infection is again, automatically integrated in a

"unique legitimate senders" database. Full support for web based email accounts in the form of domain:username:password

2) Sending via Direct SMTP: send messages directly using the MX and PTR records of the infected host's gateway

3) Sending to direct recipient

4) Sending through open relays and socks servers, both of which can provided at an additional cost

7. SET-X Mail System is highly modular, with unique features easily coded and implemented as requested by the customer

The average speed from one server is 5000/7000 emails per minute, over 1 million emails per day, and if requested you can purchase as many servers as you would like. The price of rent per month is \$2000 with additional \$1000 for each additional server if the servers are ordered at the same time."

An inside look of the system obtained on 2008-08-12 indicates that they are indeed capable of delivering what they

promise - speed, simplicity and 5000 malware infected hosts. Moreover, the attached screenshot demonstrates that 20 different email databases can be simultaneously used resulting in 16,523,247 emails about to get spammed using 52 different macroses. Furthermore, what they refer to as a dynamic set of regional servers aiming to ensure that the central server never gets exposed, is in fact fast-flux which depending on how many bots they are willing to put into "regional server mode" shapes the size of the fast-flux network at a later stage.

Spam is definitely not going away, especially nowadays when the whole process that used to require a decent investment of time and resources, has matured into an emerging market for managed service providers of spamming services whose web based interfaces successfully mimic the look and feel of anti-spam appliances. And whereas for the time being each of managed spamming services outperforms the other on different fronts, in the long-term the natural market competition forces will result in more extensive development of these systems next to the plain simple theft of intellectual property

in the form of integrating a competing system's unique features within another service.

Spammers targeting Bebo, generate thousands of bogus accounts | ZDNet

The concept of building a fraudulent ecosystem by [abusing legitimate services](#) only is nothing new, and as we've already seen numerous times throughout the year, [malicious attackers](#) are actively embracing it. Bebo, the popular social networking site is currently [under attack from spammers that are automatically registering thousands of bogus accounts](#) advertising fake online pharmacies, with the campaign owners receiving revenue through [an affiliate based program](#). The automated registration process is made possible through breaking Bebo's CAPTCHA in a combination with using bogus email registered in the very same fashion. This [isn't the first time](#) Bebo has been targeted by spammers, and [definitely not the last](#).

"Interestingly, spammers have found other uses for the valid email addresses created on sites such as MobileMe (mac.com), by linking these addresses to accounts created on social networking sites, such as Bebo. As can be seen below, a search on Google for Cialis, a drug commonly referenced in spam messages, reveals two accounts on Bebo in the top-five results returned.

Consequently, users of social networking sites are receiving more "buddy" requests from fake profiles wishing to connect. This approach works well because traditional anti-spam solutions are unable to differentiate between these requests and genuine ones. The buddy requests appear genuine as they are from the real social networking site and consequently their headers are intact and correct. Moreover, the email addresses attached to the profiles are also valid, albeit they have been created fraudulently. Often, the only visible clues may sometimes be the random arrangement of letters in the user name portion of the email address."

Approximately 30,000 bogus profiles have been generated for October alone. Why Bebo at the first place? As always, Bebo isn't targeted exclusively, but in between other social networking sites

and blogging platforms, since from a blackhat search engine optimization perspective, the more popular the abused service [the higher the visibility and shorter the timeframe for search engine crawlers](#) to pick up their bogus content. The potential for abuse here is enormous, since once the profiles start acquiring traffic, the spammers could and will easily start selling the traffic through a traffic exchange program created exclusively for malicious purposes like redirecting to live exploit URLs, and rogue security software.

Direct CAPTCHA breaking or [outsourcing the process to humans](#) in order to make such spam campaigns across social networking sites possible, is only going to get more efficient in 2009.

Spammers harvesting emails from Twitter - in real time | ZDNet

Spammers are no strangers to the ever-growing Twitter. From [commercial Twitter spamming tools](#) , to [re-tweeting trending topics](#) for delivering their message, a [new crafty search technique](#) can provide spammers with fresh and valid emails harvested from Twitter's users in real-time.

Basically, the search query consists of common phrases such as "*email me at* " and "*contact me at* " in a combination with a domain of a spammer's choice.

The result? A flood of valid and fresh email addresses of Twitter users unaware that their emails will not only get indexed by public search engines, but also, that the output can be syndicated for spamming purposes.

From theory into practice - a day after the tactic was discussed a [proof of concept script was released](#) , even though it should be logical to assume that the practice has been taking place for a while now.

Email harvesting has been around since the early days of the Internet, and has therefore greatly [evolved throughout the years](#) . From the [JS.Yamanner@m](#) worm spreading through a Yahoo Mail flaw in 2006, harvesting @yahoo.com emails from the infected indexes in order to further propagate, the [email harvesting scripts](#) crawling the web and their [modern versions](#) , to the Web 2.0 spammer's mentality of harvesting [instant messaging](#) and social networking [user names](#) - their database usually ends up as value-added service in a [managed spam vendor's](#) proposition.

In Twitter's case, their [TOS](#) states that:

You are solely responsible for your conduct and any data, text, information, screen names, graphics, photos, profiles, audio and video clips, links ("Content") that you submit, post, and display on the Twitter.com service

And whereas that should be the case, what Twitter can do to at least slow down this efficient email harvesting approach, is to either allow its users to choose whether or not they would like to have their emails/phone numbers obfuscated ([reCAPTCHA Mailhide](#)), or enforce the policy to all users.

Spammers go multilingual, use automatic translation services | ZDNet

For years spammers relied on basic mass marketing concepts in an attempt to target everyone, everywhere, thereby sacrificing quality for quantity.

Things changed, at least for some of them. Realizing the advantages of market segmentation, certain spammers started segmenting the databases of harvested or emails based on their country of origin, followed by an attempt to go local in terms of [spamming by using the native language of the prospective recipients](#).

Nowadays, spam is not just going multilingual, on demand translation services exclusively marketed to cybercriminals are prone to change the name of the game, allowing them to easily localize the messages for their upcoming malware/spam/phishing campaign to the native language of the targeted audience.

According to the just released [MessageLabs Intelligence report for July](#) , around 5% of the overall spam volume was in the native language of the targeted audience, with the majority of the messages translated using automatic services:

Globally, the majority of spam is in English, and in July around 5%, or 1 in every 20 spam messages, was in non-English language as highlighted in Figure 1. On analyzing the proportion of spam in non-English countries, the volume of English-language spam can often be much less in than English-language countries, suggesting that spammers are targeting countries correctly rather than sending all countries English language spam. For instance, in Germany 46.5% of all spam is in German and 2.5% in French. In The Netherlands, 25% of spam is in the Dutch language while in France, 53% is in French and 4% in German. In Japan, 62.3% of the spam is found to be in Oriental non-English languages and in China, this number is 54.7%.

The ongoing localization as a trend was also confirmed in [McAfee's Global S.P.A.M Diaries](#) experiment conducted in 2008 (page 12), where the same countries once again topped the charts for receiving most of the localized spam messages.

Go through related posts - [With or without McColo, spam volume increasing again](#) ; [Atrivo/InterCage's disconnection briefly disrupts spam levels](#) ; [Google: Spam volume for Q1 back to pre-McColo levels](#) ; [Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown](#) ; [Inside an affiliate spam program for pharmaceuticals](#)

Despite the easy of use and free nature of automatic translation services, their use is prone to decline due to the questionable quality of the translated messages, which could potentially undermine the efforts the spammers are putting in the first place. Cultural diversity cannot be achieved automatically, but just like everything else in the underground marketplace nowadays, the process is available as a service.

One such service which [I've been monitoring since October 2008](#) , remains active and due to its evident partnership with a particular cybercrime-facilitating community can be easily considered the de facto choice for quality-conscious spammers who care about their anonymity - the service keeps no logs for any interaction with prospective customers.

What do you think, would spammers continue using the mass marketing approach and achieve results such as [28 sales based on 350 million spam messages](#) without localization based on the [end user's old habit of clicking on spam links](#) , or would they embrace professional translation services on a large scale?

Talkback.

Spammers attacking Microsoft's CAPTCHA -- again | ZDNet

Never let a human do a malware infected host's [CAPTCHA recognition job](#) . On their way to abuse the [DomainKeys verified server reputation](#) in order increase the probability of their spam emails reaching the receipts, spammers and malware authors are once again [attempting to break Microsoft's "revisited" CAPTCHA](#) , and are able to sign up Live Hotmail accounts with a success rate of 10% to 15%, according to an assessment published by Websense today :

"Spammers are once again targeting Microsoft's Hotmail (Live Hotmail) services. We have discovered that spammers, in a recent aggressive move, have managed to create automated bots that can sign up for and create random Hotmail accounts, defeating Microsoft's latest, revised CAPTCHA system. The accounts are then used to send mass-mailings.

Early this year (2008), as reported by Websense Security Labs, spammers worldwide basis demonstrated their adaptability by defeating a range of anti-spam services offered by security vendors by carrying out the streamlined anti-CAPTCHA operations on [Microsoft's Live Mail](#) , [Google's Gmail](#) , [Microsoft's Live Hotmail](#) , [Google's Blogger](#) , and [Yahoo Mail](#) ."

10% to 15% recognition rate or *"one in every 8 to 10 attempts to sign up for a Live Hotmail account is successful "* as stated by Websense, is a bit of a modest success rate given that [the academic community has managed to achieve 92% recognition rate](#) in the past. But with hundreds of thousands of malware infected hosts, it appears that they are willing to allocate resources despite the modest success rate, and are actively spamming through the newly registered bogus email accounts.

Is machine learning CAPTCHA breaking the tactic of choice, or is the recently uncovered CAPTCHA solving economy the outsourcing model cost-effective enough to undermine the machine learning

approach? With low-waged humans achieving a 100% recognition rate and [processing "bogus account registration" orders](#) , it may in fact be more cost-effective for a cybercriminal to outsource the process, than allocating personal resources and achieving a lower success rate. One thing's for sure - CAPTCHA based authentication has been persistently under attack from all fronts, during the entire 2008.

Spam coming from free email providers increasing | ZDNet

After [analyzing three weeks of spam data](#) between June 13 to July 3, 2008, Roaring Penguin Software Inc. found

evidence that [spam originating from the top three free email providers](#) (Gmail, Yahoo Mail and Hotmail) is increasing, with spammers in favor of abusing Gmail's privacy preserving feature of not including the sender's original IP in outgoing emails :

"Spammers are increasingly using free e-mail providers to avoid IP address-based reputation systems. These systems track mail sent by various IP addresses and assign each IP address a rating. Some anti-spam software operates largely or exclusively on the basis of the IP address rating.

Roaring Penguin's data shows that over the three weeks from June 13 to July 3, 2008, the percentage of US-originated spam originating from the top 3 free e-mail providers (Yahoo, Google and Hotmail) rose from about 2% to almost 4%. Roaring Penguin believes that spammers are using Google's service in particular to send spam, relying on the fact that blacklisting Google's servers is impractical for most organizations. According to their data, the probability that an e-mail originating from a Google server is spam rose from 6.8% on June 13 to a whopping 27% on July 3."

Spammers and phishers are not just interested in the clean IP reputation of free email providers, they are also interested in taking advantage of the trust they have established among themselves through the use of [DomainKeys and Sender ID Frameworks](#) , and by abusing this through the bogus accounts that they've automatically registered by breaking the CAPTCHA based authentication, reach the widest possible audience and ensure the successful receipt of their spam/scam.

How are they managing to efficiently abuse these services, and is [CAPTCHA breaking](#) for the purpose of automatically registered bogus accounts to blame? [The broken CAPTCHAs](#) are only part of

the problem. It all starts from the basics, in this case, the companies themselves admitting there's a problem and how committed they are in not just fighting **incoming spam** , but also, **outgoing spam** .

The whole quality and assurance process applied by spammers is nothing new, in fact phishers and malware authors have been putting more efforts into coming up with easier ways to measure the return on investment (ROI) for themselves, and to present clear performance data to those taking advantage of their services. Just because someone has successfully sent several million spam emails, doesn't mean that the messages didn't got filtered, and when they did, what number exactly. Coming up with in-depth spam campaign metrics, and processes for verification of delivery, are becoming a top priority for everyone involved in this underground ecosystem.

The problem of spam and phishing coming from free email providers, has had its peaks in the past two years, prompting popular spam blacklists such as [SORBS and Spamcop to blacklist entire Gmail servers](#) due to their inability to obtain the real sender's IP. It's a signal from the anti spam community, and since Gmail will continue not revealing the real sender's IP, something they've received a lot of criticism from anti spam vendor, but a lot of applause from privacy fighters, the best they can do is balance their incoming VS outgoing spam fighting strategy. Here's a comment from [an anti-spam vendor commenting on the problem back in 2006](#) :

"Gmail has taken an extreme position on privacy that inhibits the antispam community from doing their job, and it's ticking people off," says Tom Gilles, co-founder of IronPort. **Some 10% to 15% of the spam IronPort sees comes from free Web-mail accounts, too big a slice to turn a blind eye to** . "From time to time, Gmail mail is getting blocked because spam is leaking out of their service," Gilles says. "Sometimes the babies get thrown out with the bath water, and that is the rub.

It's difficult to gauge how widespread the problem of missing Gmail is, since no blocking records are available, though experts worry it's growing along with the Gmail service. Gmail had 6.7 million visitors in February, up 4.1 million from a year ago, according to

measurement firm comScore Networks, a jump that suggests lost email has yet to hurt the service's growth. Yahoo Mail is still nearly 10 times bigger, hosting 64.6 million visitors last month, and AOL and Hotmail are also orders of magnitude larger. The situation reveals again how the studiously iconoclastic search engine is wrangling with where to draw the line on Internet privacy. As in other recent cases, Google is taking a harder line than its peers."

Moreover, the abuse of the authentication at these free email providers, by either breaking the CAPTCHA images automatically, or outsourcing the process to human CAPTCHA breakers who earn cents to authenticate the registration process for the spammers to abuse, is clearly making an impact. For instance, underground services offering hundreds of thousands of pre-registered bogus accounts are popping up like mushrooms these days, and their maturity into a customer-tailored proposition offering everyone the possibility to pre-register bogus accounts at services and web sites that they are not currently targeting, speaks for the confidence they've built into their ability to deliver the goods. The most recent one which I covered in a previous post is continuing to automatically pre-register accounts with its inventory emptying and filling itself automatically in between the customer's feedback indicating the quality of the service. Here's a sample of their inventory as of the last five minutes :

Yahoo.com - 270,565 pre-registered accounts
Hotmail.com - 167,013 pre-registered accounts
Gmail.com - 159,892 pre-registered accounts

These is just the tip of the iceberg, with many other such services offering different inventories and using different tactics in the registration process. And while the companies themselves are keeping track of the latest developments in this ongoing abuse of their services, it's all a matter of drawing the line at a particular moment of time. For instance, a known to be malware infected IP that has repeatedly attempted to send hundreds of thousands of phishing and spam emails on behalf of the botnet it participates in, shouldn't be trusted in any authentication or registration attempts if you're to take the radical approach, or have the end user warned

about what's going on and why is she [not allowed to use the site's services unless action is taken](#) . The point is that, preventing automatic authentication abuse as a process is very similar to preventing click fraud, and fighting spam in general with the only different in the shift of perimeters from applying the techniques on incoming emails, to the authentication process in general.

Most of the human CAPTCHA breakers, and the automated programs will either abuse [malware infected hosts as open proxies, or use open proxy lists in order to change their IP on every several registrations](#) . Considering that the majority of malicious activity comes from well known bad parties are often blocked by default at the email gateway without even bothering to inspect the content in email messages coming from their networks/IPs, the same approach, activity from malware infected hosts should be challenged more aggressively than it is for the time being.

The increasing spam and phishing emails originating from legitimate email service providers is prone to increase, and fighting incoming spam should be balanced with fighting outgoing spam. Moreover, email spam is so Web 1.0, that the possibilities for abusing the joys offered by Web 2.0 services are slowly starting to materialize, with spammers being a step ahead of the filtering solutions.

Spam attack shut downs Marshall Islands email service | ZDNet

Marshall Islands [National Telecommunications Authority](#) is reporting that a sustained spamming attack during the past 24 hours managed to cause a successful Denial of Service attack on the email services of the islands only Internet Service Provider. [More info on the attack](#) :

More than 18 hours after the initial attack Tuesday incoming email service to the monopoly provider had still not been restored. The government-owned National Telecommunications Authority (NTA) was hit with a sudden four-fold increase in incoming email, which it described as an attack by "zombie computers", said an NTA spokesman. While NTA customers could send and receive emails to each other through the local system, virtually no non-NTA emails had been received since Monday, impacting local businesses, banks and government offices.

Is this coordinated spamming attack is someone's way to ruin the monopoly of the islands' only Internet Service Provider by emphasizing on how centralization and monopoly is a disadvantage to the final customer, or is it a sudden peak of bandwidth wasting image spam as usual? It surely demonstrates that a single ISP per country, no matter if it's a third world country or a popular tourist destination, make the whole country's Internet infrastructure easier to shut down and censor. Take [Zimbabwe](#) and [Burma](#) for instance.

South Korea to block port 25 as anti-spam countermeasure | ZDNet

[South Korea](#) is considering a [nation wide block of port 25](#), as a anti-spam countermeasure aiming to reduce the volumes of spam affecting the country.

The ban, set to go in effect as of December, will replace [port 25](#) with port 587 and 465 for SMTPS.

Why is this initiative prone to fail?

Mostly because of the way modern malware and spam networks operate. For instance, modern malware has built-in SMTP engines that are port-independent. Moreover, geolocated and malware-infected hosts within South Korea could be automatically updated using the new specs in a matter of seconds, once again continuing the abuse of legitimate networks, while playing by the newly introduced rules.

[Spamming through web-based email](#) is yet another way for cybercriminals to bypass the newly introduced regulations. Once the CAPTCHA-solving process for [popular free web-based email providers](#) has been outsourced to [Indian providers of CAPTCHA-solving services](#), thousands of newly registered emails will be automatically used for outgoing spamming purposes, once again successfully bypassing the newly introduced regulation.

What do you think? Would the blocking of port 25 reduce the levels of spam significantly, or is the initiative prone to fail?

Talkback.

Source code for Skype eavesdropping trojan in the wild | ZDNet

Earlier this week, Swiss programmer Ruben Unteregger who has been reportedly working for a [Swiss company ERA IT Solutions](#) responsible for coding government sponsored spyware, has released the [source code of a trojan horse that injects code into the Skype process](#) in order to convert the incoming and outgoing voice data into an encrypted MP3 available at the disposal of the attacker.

Here's [how the trojan](#) , currently [detected](#) as [Trojan.Peskyspy](#) , works:

"When the Trojan is executed, it injects a thread into the Skype process and hooks a number of API calls, allowing it to intercept all PCM audio data going between the Skype process and underlying audio devices. Note: Since the Trojan listens to the data coming to and from the audio devices, it gathers the audio independently of any application-specific protocols or encryption applied by Skype when it passes voice data at the network level.

Note: The incoming and outgoing audio data are stored in separate .mp3 files. The Trojan also opens a back door on the compromised computer, allowing an attacker to perform the following actions: - Send the .mp3 to a predetermined location - Download an updated version - Delete the Trojan from the compromised computer"

Skype is often dubbed a "[national security threat](#) " by governments all across the globe due to their -- at least publicly acknowledged -- inability to [crack the 256-bit encryption VoIP calls](#) .

And while some of these governments are reportedly spending surreal amounts of tax payer's money ([Rental of the Skype-Capture-Unit per month and instance EUR 3.500](#)) in order to achieve their objectives, others are taking the cost-effectiveness path by [attacking the weakest link in the process](#) - the end user infected with a targeted DIY government sponsored spyware recording all ongoing

and incoming Skype calls, thereby bypassing the need to attack the encryption algorithm.

Source code for ikee iPhone worm in the wild | ZDNet

Following last week's [systematic exploitation of jailbroken iPhones in the Netherlands](#) through a technique originally [discussed in 2008](#) , a 21 years old opportunist has recently [launched the first iPhone worm](#) , this time targeting customers of Australian mobile carriers.

Upon successful exploitation of devices running SSH with default passwords, the worm would announce its presence by changing the wallpaper to a new one featuring pop-star Rick Astley.

Despite the author's intention to raise awareness on the issue, the originally released as "closed source " code for the "awareness-building worm" has now leaked in the wild, with several modifications already capable of stealing a compromised iPhone's contacts and SMS messages.

In an interview published with the [author of the iPhone worm](#) , he states that his iPhone alone has already infected 100+ devices, and commented that international propagation "*would have been sheer luck* ", since "*the code itself is set to firstly scan the 3G IP range the phone is on, then Optus/Vodafone/Telstra's IP Ranges (I think the reason Optus got hit so hard is because the other 2 are NAT'd) then a random 20 IP ranges. I'm guessing a few phones hit a range that another vulnerable phone was on*" .

Interestingly, in a [recent poll results](#) , 76% of the people who voted believe that "*He's done iPhone users a favour. This was an acceptable way to raise awareness of poor security*". I wonder what would their attitude be if they knew that several modifications and customized modules are already capable of stealing their SMS messages and contacts, potentially using them for fraudulent activities.

What do you think, did the teenagers that launched these attacks during the last two weeks did someone a favor, or did they actually started a short-lived trend with malicious copycats already looking for

ways to exploit the potentially hundreds of thousands of jailbroken devices using the easy to find 3G IP ranges?

TalkBack.

Sopelka botnet drops Citadel, Feodo, and Tatanga crimeware variants | ZDNet

Security researchers from S21sec have published [an analysis of the Sopelka botnet](#). Operating since May 2012, it is known to have launched five unique campaigns, three of which dropped crimeware variants from multiple families.

Based on the researchers' data, the group behind the botnet managed to infect over 16,000 hosts, the majority of which were geolocated to Germany and Spain, the two countries topping the infection per countries chart.

Just how easy is it to develop and manage such a botnet for the sake of monetizing the infected hosts, and [cashing out](#) in complete anonymity? In 2012, the process of developing and managing such a botnet is entirely automated, efficient, and most importantly - available as a service through [a malicious underground Cybercrime-as-a-Service provider](#).

Sopelka is a typical representative of the "[botnets that never make the news](#)" category. Small, resilient, these botnets usually go [beneath the radar](#) until their payload starts attracting the attention of vendors and researchers.

What's also worth emphasizing on regarding this type of "[aggregate-and-forget](#)" botnets, is the fact that they plan a crucial role in the ongoing cyber warfare arms race, allowing their operators to launch a multitude of cyber operations, and achieve a complete plausible deniability thanks to the way these botnets were used.

What do you think? Will the future of cyber warfare be dominated by small and targeted botnets, or will it be dominated by good old fashioned massive botnets? Would botnets even count in comparison to targeting a single individual through sophisticated social engineering and technical means?

TalkBack!

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Sony PlayStation's site SQL injected, redirecting to rogue security software | ZDNet

The latest high trafficked web site to fall victim into the continuing waves of massive SQL injection attacks courtesy of

copycats and the ASProx botnet, is Sony's [PlayStation U.S. site](#) according to a recent post at [SophosLabs's blog](#) :

"Researchers at IT security firm Sophos have warned lovers of video games that pages on the US-based Sony PlayStation website have been compromised by hackers. Experts at SophosLabs have discovered that cybercriminals have successfully used an SQL injection attack to plant unauthorized code on pages promoting the PlayStation games "SingStar Pop" and "God of War".

At the time of writing the hacker's code attempts to dupe web surfers by running a fake anti-virus scan and displaying a bogus message that their computer is infected with a variety of different viruses and Trojan horses. The hackers' aim is to scare unsuspecting computer users into purchasing a bogus security product. Sophos warns, however, that it would be trivial for the hackers who have compromised the webpages to alter the payload so that it became more malicious, and installed code designed to turn Windows PCs into a botnet or to harvest confidential information from users. "

Sony PlayStation's site hasn't been hacked, it's been abused as a redirector to a malicious site serving rogue security software while participating in a SQL injection launched by Chinese hackers. Moreover, it's important to point out that, Sony's PlayStation site hasn't been on purposely targeted, it's been targeted automatically in between the rest of the [794 domains SQL injected](#) with the same domain - **coldwop .com** . Let's get down the bottom of this campaign.

The number of SQL injected sites with this domain is close to 39,000, and I'm in fact surprised that for the time being the

domain is down, given that it was using a multi-layered fast-flux infrastructure with over a hundred different IPs associated with it and rotating with others every three minutes. As for the Playstation.com, there are 209 pages that have been SQL injected for the being. Who's behind it? The [automated SQL injecting approach courtesy of the ASProx botnet](#) , a botnet's that's increasingly multitasking next to the rest of malicious activities it's responsible for.

The botnet masters are continuing to put efforts into ensuring the survivability of their campaigns. In the previous ones they were injecting a single malicious domain on as many vulnerable sites as possible. These days, I'm coming across over 5 different injected domains on a single site, all of which are naturally in a fast-flux. This attack optimization approach clearly indicates that the botnet masters are keeping track of the success rates of their campaigns, and are applying metrics to assess them.

If you don't take care of your web application vulnerabilities, someone else will.

Related posts:

- [Over 1.5 million pages affected by the recent SQL injection attacks](#) - [Redmond Magazine Successfully SQL Injected by Chinese Hacktivists](#) - [200,000 sites spreading web malware, China's hosting the most](#) - [Google introducing Safe Browsing diagnostic to help owners of compromised sites](#) - [Microsoft ships free code auditing tools to thwart SQL injection attacks](#)

Sony Europe hacked by Lebanese grey hat hacker | ZDNet

A grey hat hacker known as idahc, has managed to compromise Sony Europe's Database of Application Store.

The SQL injection hack has revealed 120 credentials, including the username, password, mobile, office, email, and website of the affected users -- all in plain text. Last week, the same hacker has once again managed to compromise ***ca.eshop.sonyericsson.com*** , with the hacker claiming that he had the ability to extract credit cards data, but didn't do it since he doesn't perceive himself as a black hat.

Snow Leopard's malware protection only scans for two Trojans | ZDNet

The much hyped built-in [malware protection](#) into [Apple's Snow Leopard upgrade](#) appears to be nothing more than a [XProtect.plist file](#) containing [five signatures](#) for two of the most popular Mac OS X trojans - [OSX.RSPlug](#) and [OSX.Lservice](#) .

Intego, the company that originally [reported the new feature](#) , has just released a [comparative review](#) of their (commercial) antivirus solution next to Apple's anti-malware function. Here are some of the highlights:

Apple's anti-malware function only scans files downloaded with a handful of applications (Safari, Mail, iChat, Firefox, Entourage, and a few other web browsers) -- therefore the disturbingly modest signatures base would be undermined if the user were to download the malware from a BitTorrent application

Apple's anti-malware function currently only scans for two Trojan horses, as of the initial release of Snow Leopard -- relying on such a modest set of signatures for malware variants of known OS X families, clearly indicates the premature release of the feature

Apple's anti-malware function receives occasional updates via Apple's Software Update -- in respect to malware, even Mac OS X malware, every modified variant of a known malware family enjoys a decent life cycle until it gets detected through malware signatures. In its current form the reliance on occasional Apple Software Updates compared to regular/scheduled independent signatures update, clearly increases the life cycle of a known piece of malware

Go through related posts: [New Mac OS X DNS changer spreads through social engineering](#) ; [Mac OS X malware posing as fake video codec discovered](#) ; [New Mac OS X email worm discovered](#) ; [Trojan exploiting unpatched Mac OS X vulnerability in the wild](#)

It its current form, Snow Leopard's anti-malware feature offers nothing else but a false feeling of security. What do you think? Talkback.

Skype vouchers themed site serving client-side exploits and malware | ZDNet

Looking for Skype vouchers? Bargain deals?

Make sure you don't land on skypevouchers(dot)com.

According to security researchers from GFI Labs, the typosquatted domain is [currently serving client-side exploits and malware](#) to its visitors.

The malware is served via a tiny iFrame tag, loading the legitimate manjakuhappy(dot)com web sites, which has been compromised to participate in the malicious campaign. The domain is serving [CVE-2011-3544](#), with the following MD5's corresponding the exploits served at the site: **MD5: d3f933524c85c96a76f7ffd516d335c0** served from halloffam(dot)bee(dot)pl, and **MD5: 58db6e6e25d9b8e4742f2ef9b43c3818** served from themettco(dot)bee(dot)pl.

End and corporate users are advised to ensure that they're using the Internet with the [latest versions of their third-party software](#) and [browser plugins](#).

Skype patches security policy bypassing vulnerability | ZDNet

In a [security bulletin issued two days ago](#) , Skype's latest version fixes a [File URI Security Bypass Code Execution](#)

[Vulnerability](#) originally reported by Ismael Briones :

Remote exploitation of a security policy bypass in Skype could allow an attacker to execute arbitrary code in the context of the user.

The "file:" URI handler in Skype performs checks upon the URL to verify that the link does not contain certain file extensions related to executable file formats. If the link is found to contain a blacklisted file extension, a security warning dialog is shown to the user. The following file extensions are checked and considered dangerous by Skype; .ade, .adp, .asd, .bas, .bat, .cab, .chm, .cmd, .com, .cpl, .crt, .dll, .eml, .exe, .hlp, .hta, .inf, .ins, .isp, .js.

Due to improper logic when performing these checks, it is possible to bypass the security warning and execute the program. First of all, checking is performed using a case sensitive comparison. The second flaw in this check is that the blacklist fails to mention all potential executable file formats. By using at least one upper case character, or using an executable file type that is not covered in the list, an attacker can bypass the security warning.

Basically, while a link including .exe would trigger a warning message for potentially malicious file, a link including .exE wouldn't. Affected are all Skype Windows clients prior to and including 3.8.*.115, with the vulnerability already fixed in versions 3.8.0.139. How effective is the blacklisted executable file extensions filter in general? Let's say not as effective as it used to be couple of years ago when the end users were advised not to click on executable files, and avoid visiting suspicious sites. Nowadays, [legitimate web sites](#) are increasingly serving malware through their [susceptibility to SQL injection](#) , and links to what looks like image files distributed over IM networks on behalf of malware attempting to infect new hosts, are nothing more but [redirectors to the live exploit URLs](#) .

Modern malware authors are also fully aware of the "executable file extensions" blocking mentality, in fact the majority of free services offering web space do not allow uploading of executable files in order to at least theoretically prevent the abuse of their services to host and spread malware. Malware authors adapt by bypassing the block and host the malware in a .jpg image file extension which later one gets locally saved on the infected machine as an executable file. Here's an example of a spoofed executable file **festaaqui .com /img/ gmillogof.jpg** , and despite that it's visually looking as an image file, 23 out of 32 antivirus scanners already detect its real intentions (TrojanSpy.Banker) which in this case are to steal your E-banking details.

Considering the existence of [nasty vulnerabilities](#) allowing [code execution](#) while processing [malformed image files](#) or other types of [video multimedia](#) , one should consider breaking out of the dangerous executable file extensions stereotype, and look beyond the file extension.

Silent security updates coming to Apple's OS X Mountain Lion | ZDNet

[According to AppleInsider](#), in the latest update to the Mountain Lion Developer Preview, includes the "OS X Security Update Test 1.0" feature, which will run daily or whenever a Mac restarts in an attempt to silently download and install the latest security updates.

In June, 2012, Apple also introduced [silent patching for Adobe Flash Player](#) running on Mac OS X.

Although for the time being we're not seeing an epidemic growth in Mac OS X malware, due to what I believe is lack of mature monetization models offered by affiliate networks, this will inevitably change in the long term with cybercriminals looking to compromise more users with high purchasing power.

Mountain Lion Developer Preview users are advised to apply the update immediately in order to take advantage of the new feature.

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Should a targeted country strike back at the cyber attackers? | ZDNet

On a regular basis, [political sentiments over the use of kinetic/nuclear weapons](#) or [offensive cyber warfare capabilities](#) against [cyber adversaries](#), reemerge internationally, as a [desperate response to the threat](#), largely based on the outdated situational awareness of the person making them.

The situation becomes even worse when these people are either directly participating in the chain of command for a particular country, or have political bargaining power that can undermine the common sense brought in by those in the trenches of cyber operations.

Excluding the political sentiments, attempting to use a kinetic force against a physical targeted believed to be the location of the cyber attacker, as well as Denial of Service (DoS) attacks, is a very bad idea.

Let's discuss some of the key trends in the market for offensive cyber warfare tools, as well as two fully realistic scenarios, undermining the the effectiveness of frontal cyber warfare engagement tactics.

The commercialization of offensive cyber warfare tools

Like in any other market, [demand always meets supply](#). In the case of offensive cyber warfare, the supply is largely driven by a military principle known as the "[necessity and proportionality](#)", combined with a particular government's interest in doing the single most logical thing a targeted country thinks it should do - should it strike back at the cyber attackers, and what kind of tools should it rely on?

In 2004, a [risk metrics company started promoting](#), perhaps for the first time ever, a commercial [offensive cyber warfare solution](#), described as:

The first IT security solution that can both repel hostile attacks on enterprise networks and accurately identify the malicious attackers in

order to plan and execute appropriate countermeasures – effectively fighting fire with fire. “While other companies offer only passive defense barriers, Symbiot provides the equivalent of an active missile defense system.

According to their press release, the product development was undertaken, following the [anticipation of this emerging market segment](#). Years later, another vendor introduced a mainstream offensive cyber warfare platform. [Rsignia's CyWarfius CyberScope](#) :

The CyWarfius CyberScope is an offensive capable cyber weapon specifically designed to address the unique requirements of the cyber warrior. With the ability to conduct a surgical offensive strike on a specific target, the CyberScope is the first offensive tool of its kind to provide pseudo-kinetic countermeasures against cyber threats.

These commercial, off-the-shelf propositions, are a also a direct response to public statements, and [comments made in regard to the use of kinetic/offensive made by U.S defense officials](#) throughout the years.

With more countries showing interest in the practice, due to the high volume of cyber attacks hitting their infrastructures experience on a daily basis, it's important to highlight some of the scenarios that have the power to undermine such offensive doctrines.

Compromised legitimate infrastructure acts as a "virtual human shield"

Assuming that a target country decides to strike back at the cyber attacker's infrastructure used in the attack, the fact that it may well be striking back at legitimate infrastructure, is fully realistic one, since in 2009, [71 percent of the Web sites with malicious code were legitimate](#).

Moreover, throughout the entire 2009, cybercriminals once again demonstrated the same "virtual human shield" concept, by blending legitimate infrastructure into the malicious mix, with notable examples including the abuse of legitimate services such as, [Twitter](#)

, [Google Groups](#) , [Facebook as command and control servers](#) , as well as [Amazon's EC2 as a backend](#) .

The problem with striking this infrastructure, is that from a military perspective, it's a civilian target. The use of "human shields" in this case a "virtual human shield", has been a major [legal and ethical consideration in every conventional military conflict](#) where such tactics were used.

And even if the direct impact on a third country's compromised infrastructure is legally considered as a collateral damage, the existence of this practice leads to the establishment of the foundations for launching false flag cyber operations.

False flag cyber operations impersonating a particular country

Remember the infamous "[On the Internet, nobody knows you're a dog](#)." cartoon? Or the [War Games movie](#) ?

In the context of cyber warfare, in 2010 nobody knows you're Burkina Faso online, and yes, even North Korea. In the wake of the [Google-China cyber espionage saga](#) , everyone put the spotlight on China due to its internationally recognized cyber espionage doctrine throughout the past couple of years.

However, no attention was brought to the fact, that the campaign, including [many of the ones that were profiled](#) at a target stage, could have been [false flag cyber operations](#) , launched by another country, or even an individual/group of individuals, engineering cyber warfare tensions relying on the negative reputation of the "usual suspects".

The concept of false flag cyber operations is anything but a new one. Since the early appearance of botnets, the people behind them realized that they could easily hijack a country's online reputation, by exclusively using only infected hosts within that country for [launching attacks](#) , or [anonymizing their activities](#) by using them as "[stepping stones](#) ", a practice also known as "[island hopping](#) ".

In Google-China's cyber espionage campaign, the smoking gun was a hacked server based in Taiwan, including several other based in the U.S. And even though there was to direct connection between

the campaign and China's infrastructure, the fact that as I'm posting this article, several hundred Chinese government subdomains are compromised, and serve client-side exploits to their visitors, easily turns them into playground's for a foreign intelligence agency, or anyone else wanting to impersonate the country online.

Related posts: [Attack of the Opt-In Botnets Coordinated Russia vs Georgia cyber attack in progress Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites 'Anonymous' group attempts DDoS attack against Australian government](#)

From a CYBERINT (cyber intelligence) perspective, given that enough international cooperation is taking place, the Internet can be a pretty small place for every attacker or cybercriminal in general. However, in terms of attributing the real source of a cyber attack, the evidence obtained may be exactly the evidence a third-party may want you to see.

Therefore, attempting to launch offensive cyber warfare tactics, or increasing the political pressure against the adversary a particular country is tricked into believing is responsible for the attacks, is clearly what a third country may want to achieve.

Cyber warfare tactics undermining the offensive cyber warfare capabilities of the targeted country

Two of the many cyber warfare tactics made possible these due to the maturity of cybercrime concept into today's [Crimeware-as-a-Service \(CaaS\) business model](#), can easily turn offensive cyber warfare capabilities such as counter strike DDoS attacks, completely obsolete. For instance:

Country A (Russia) knows that country B (United States) would DDoS back anyone. It hates country C (China), so it rents bots within country C (China) to DDoS country B (United States). Ultimately, B (United States) DDoS-es C (China) - This tactic demonstrates the problem with publicly acknowledging your ambitions to strike back at cyber attackers, theoretically even nuke them. And although, connections to known cybercrime-friendly groups were established for their participating in renting botnets to some of the high-profile cyber attacks ([Russia vs Georgia as an](#)

[example](#)), the people behind these services closely monitor the attribution patterns applied by the community. This proactively monitoring of mitigation strategies, helped them embrace the so called "[aggregate-and-forget botnets](#)", where a certain botnet is uniquely aggregated, in order to make harder, if not virtually impossible to trace it back to a particular group.

Country A (China) wants to undermine the offensive DDoS capabilities of country B (Russia). It DDoS-es from bots located within country B (Russia). If B (Russia) starts DDoS-ing back the cyber attackers, it would ultimately end up DDoS-ing its own infrastructure - One of the most interesting questions that this tactic leaves unanswered is - how is a targeted country going to respond to a large scale denial of service attack, which is coming from malware-infected hosts within the targeted country itself? One of the most recent examples of this concept, was the "[Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites](#)" campaign, which was so successful in terms of the internal traffic generated by the protesters, that discussions to stop the DoS attacks in order to allow the upload of user generated content started taking place. Basically, the Iranian government was heavily hit by the same tool that it was using to spread it's own "version of the story". Taking it offline in order to prevent the leak of disturbing material to the rest of world, means denying themselves the ability to influence foreign opinion as well.

What do you think?

How should a targeted country threat the infrastructure used by the cyber attackers, even if it's a compromised third country's servers they are using? Should a targeted country use its offensive cyber warfare capabilities as a bargaining power against a particular cybercrime-tolerant country, even through the attacks are launched by someone else?

Also, how would a targeted country strike back at a country that has virtually no Internet infrastructure at all?

TalkBack, and share your opinion.

Images courtesy of [GameSpot "World of Conflict"](#) , [U.S Air Force Cyber Command \(Provisional\) Public Affairs](#) , and [War Games, the](#)

movie .

Seven myths about zero day vulnerabilities debunked | ZDNet

Another month, another zero day flaw has been reported, with malicious attackers logically taking advantage of the window of opportunity, by launching malware serving attacks using it. With vendor X putting millions of users in a "*stay tuned mode* " for weeks, sometimes even longer, the myths and speculations surrounding the actual applicability of zero day flaws within the cybercrime ecosystem, continue increasing.

Are zero day flaws what the bad guys are always looking for? Just how prevalent are zero day flaws within their business model? Are zero day flaws crucial for the success of targeted attacks attacks?

Let's debunk seven myths about zero day flaws, using publicly obtainable data, an inside view of the cybercrime ecosystem, and, of course, common sense like the one malicious attackers seem to possess these days.

Zero day flaws are the primary growth factor of the cybercrime ecosystem - Not even close. In 2010, the cybercrime ecosystem is largely driven by the millions of end users and companies using the Internet with outdated third party applications, and plugins. With the current trends shifting from the exploitation of OS-specific flaws, to the exploitation of client-side vulnerabilities, or [good old fashioned social engineering attacks](#), the rather myopic perspective of the end user/company towards the current threatscape, results in the success of malicious attackers in general. Then, if it's not zero day flaws that the bad guys rely on, what is it that drives their business model? The [lack of security awareness internationally](#), resulting in good [click-through rates](#) given they systematically rotate the social engineering themes, the high number of [insecure applications/plugins](#) running on an [average Internet-connected PC](#), as well as the current [DIY or Cybercrime-as-a-Service](#) state of the ecosystem, allowing [unsophisticated attackers to have access to sophisticated attack tools](#), all

contribute to growth of the ecosystem.

Zero day vulnerabilities is what the cybercriminals are looking for all the time - If they truly were, the cybercrime ecosystem would have never matured into the efficient money machine it has become today. How come? Basically, what the bad guys suddenly realized is that, not only is there a high probability that given enough traffic is hijacked, a huge number of users would be exploitable, but also, that the time and resources they would have spend finding zero day flaws, could be invested somewhere else. This marginal thinking to some, or Keep It Simple Stupid (KISS principle) to others, is what is currently driving their business model - acting based on the harsh reality, instead of conceptualizing on how a perfect(ly) (patched) world is supposed to look like. The myth that zero day vulnerabilities is what the bad guys are after all the time, comes from the concept of [the black market for zero day vulnerabilities](#), a market which has greatly evolved from what it was a few years ago. From OS-specific, to client-side specific, today's pragmatic nature of this market is orbiting around the exploitation of web applications. The only reason why the bad guys have shifted their interests is thanks to the realizations made in point one, namely, now that they are aware that [millions of users are susceptible to outdated flaws](#), targeting popular web applications which would allow them to launch mass SQL injection/or application-specific attacks, consequently hijack the traffic, is [what they're currently interested in](#).

Zero day flaws are crucial for the success of targeted attacks/advanced persistent threat campaigns - Although zero day flaws appear to be cornerstone for a successful intrusion inside a high profile network, which is presumably better secured than the PC of the average Internet use, numerous cases show otherwise. Perhaps one of the most recent and widely discussed such case, is [the Google-China espionage saga](#). Think malicious attackers, in order to anticipate malicious attackers. Why didn't they try discovering a vulnerability in Google's own browser, Chrome, which should have been the company's logical browser choice in the first place. Intelligence gathering on the fact that there's an IE6 running on a PC, for sure. However, what I'm trying to imply is that there's a high probability that the very same PC which was running Internet

Explorer 6, could have also been exploited using ubiquitous flaws found in Adobe's products. How come? It's the insecure mentality, lack of enforced security auditing which would have prevented IE6 running on one of Google's hosts in the first place. As far as targeted attacks/advanced persistent threat type of campaigns are concerned, on a quarterly basis a malicious gang that's clearly interested in infecting high-value targets, redistributes a [**ZeuS crimeware serving campaign, using exclusively .gov and .mil themed subjects**](#). What's so special about these campaigns in the context of zero day flaws, is that they rely on the manual interaction of the targeted user with the binary hosted on a compromised site, and not on zero day flaws. Although zero day flaws are "desirable", from my perspective they're not crucial for the success of targeted attacks.

Operating system specific flaws are more widely exploited than 3rd party application/plugin flaws - Exactly the other way around. According to the SANS Institute's 2009 Top Cyber Security Risks report, [**application patching is much slower than operation system patching**](#), although client-side vulnerabilities dominate the cyber threat landscape. Microsoft's own [**Security Intelligence Report Volume 8**](#), also points out that based on their data, third party flaws are more widely exploited than Windows OS specific flaws. Similar conclusions can be drawn by looking at [**BLADE Defender's Labs real-time infection data**](#), in particular the application targeted, and not the browser targeted. Moreover, the susceptibility of exploitation is one thing, the actual infection rate is entirely another. Case in point, Secunia's recently released report indicates that [**Apple had the most vulnerabilities throughout 2005-2010**](#). And even if we exclude the obvious differences between Mac OS X's market share compared to market share of Microsoft Windows, theoretically Apple's users are supposed to under constant fire from all angles. Why aren't we seeing this trend? Pretty simple, what the vendor/application centered, to "target them all" exploitation tactic executed by the bad guys has shown us, is the harsh reality, namely the success of their infection rates are not based on the vendor/product with the most flaws, but on the lack of patching on behalf of the end users. Basically, even if the users of a

vendor with a relatively modest vulnerabilities count aren't patching, or the vendor doesn't have a well developed communication channel, these users will pop-up as successful infections. Hence, the difference between being vulnerable as vendor, and getting actively exploited thanks to your unpatched users, next to the flawed communication model with them.

Once a patch for a particular flaw is available, case's closed -

One of the most common myths about zero day flaws, is that, once the patch has been released, it's end of story for the vendor as it has now responsibly taken care of the vulnerability. The lack of prioritization of the second stage in the process, namely, communication next to [the WGA-wall](#), results in the current situation, where [one of the world's largest botnets, Conficker](#), continues adding new hosts, despite the fact that a patch has been released. The same situation can be seen with multiple vendors, whose users doesn't have a clue that they're getting themselves infected through flaws which have been patched half an year ago. This lack of second stage communication, can be best seen in [Mozilla Foundation's admirable efforts](#) to protect the end user from himself, with such initiatives such as the [Plugin Check](#) which also offers plugin checks for users of competing browsers. If only was the same [socially-oriented mentality](#) applied by high-trafficked web sites, which compared to anyone else, are in a perfect position to make an impact on a large scale, from a security awareness perspective.

Full disclosure, in order to motivate a vendor to patch the flaw benefits the community and its users -

Although practice has shown that this approach acts as an incentive for vendors to start prioritizing the existence of a flaw, which they have previously denied, the flawed communication model between the vendor and its users discussed in point five, undermines this myth. How come? Pretty simple. The end user who's been using the Internet with outdated 3rd party applications and browser plugins for half an year, will continue doing so, even through they will perceive themselves as "Patch Tuesday" aware. They will also continue being victim of the [over-expectations put in the effectiveness](#) of antivirus solutions, forgetting that [prevention is better than the cure](#). This lack of DIY

"software asset management" beyond the operation system, or security awareness on the existence of the most widely abused infection tactic by the bad guys, helps them efficiency infect tens of thousands of new users on a daily basis.

Zero day flaws play a crucial role in the exponential growth of data breaches - According to [Verizon's most recent Data Breach Investigations Report](#), things are in fact even more interesting than that. The report states that based on their data sample, *"there wasn't a single confirmed intrusion that exploited a patchable vulnerability"*. So how are the bad guys compromising these networks/servers, resulting in the exposure of hundreds of thousands of sensitive records? By keeping it simple, [targeting the insecurely configured web applications](#), using customized malware, or basically doing everything else, but emphasizing on the discovery and use of zero day vulnerabilities to achieve their goals.

In no way does this post aim to disqualify the value of a zero day vulnerability to a potential attacker, or even a cyber spy. Instead, it aims to offer an objective perspective into the fact that, the cybercrime ecosystem continues to thrive without the need for zero day flaws, and it will continue to as long as millions of end users continue getting exploited with 6+ months old flaws.

Did I forget to mention a particular myth? Do you agree, or disagree with some of the points made, and what's your perspective on the myth/speculation in question?

TalkBack.

Image courtesy of [Microsoft's Security Intelligence Report Volume 8 report](#).

Security researcher finds major security flaw in Facebook | ZDNet

A security researcher has discovered a major security hole affecting the most popular social networking site, Facebook.

Basically, the [researcher found a way to upload executable files](#) -- such as those most commonly used by malicious software -- on the social network site for potential sharing. Needless to say that the potential for abuse by malicious attackers is pretty evident.

More details:

When using the Facebook 'Messages' tab, there is a feature to attach a file. Using this feature normally, the site won't allow a user to attach an executable file. A bug was discovered to subvert this security mechanisms. Note, you do NOT have to be friends with the user to send them a message with an attachment.

Is the ultimate distribution of executable files the cornerstone for distributing malware across the social networking sites? Not at all. Cybercriminals often rely on innocent-looking links that [redirect to client-side](#) exploits [serving domains](#) for achieving their objectives.

The researcher notified Facebook on 09/30/2011 and received a confirmation of his findings on 10/26/2011.

UPDATED: Facebook's Security Manager **Ryan McGeehan** had this to say:

This finding will only allow one user to send an obfuscated renamed file to another Facebook user. The proof of concept, as is, would not execute on a recipients machine without an additional layer of social engineering. Beyond that, we are not going to rely solely on string matching as a protective measure, since zip files and other things could also have unpredictable behaviors when sent as an attachment.

We are AV scanning everything that comes through as a secondary measure, so we have defense in depth for this sort of vector. This puts us at a similar level of protection as most webmail

providers who deal with the similar risk, and this finding is a very small part of how we protect against this threat overall. At the end of the day, it is more practical for a bad guy to hide an .exe on a convincing landing page behind a URL shortener, which is something we've been dealing with for a while.

Security flaw found in Amazon's Kindle Touch | ZDNet

Security researchers from heise Security have created a proof-of-concept code for a [remotely exploitable security vulnerability affecting Amazon's Kindle Touch 5.1.0 firmware](#).

The demo allows arbitrary shell commands to be injected into a Kindle Touch, allowing the security researchers to create a script where the Kindle sent back a copy of `/etc/shadow` to a heise Security web server.

Apparently, the [security issue has been known for over three months](#) now. Amazon Inc. responded to heise Security that they're working on a patch. Unfortunately, the patch cannot be pushed to Kindle Touch users and they would have to personally issue the update on their devices.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Security breach hits DivShare, unauthorized access to its database | ZDNet

The popular document and media sharing service [DivShare](#) , suffered a security breach according to a security announcement [posted by DivShare's support team](#) earlier this week :

Late last night we were alerted of a security breach that allowed a malicious user to access our database, which included user e-mail addresses and other basic profile information. **No financial information has been accessed by any unauthorized parties.** We have taken extreme measures to secure the site in the last 12 hours and are currently in the process of rolling out new security precautions, which is why many files are currently unavailable. We apologize for this inconvenience and for the oversights that allowed this security breach to take place. We take the security of all data and files very seriously and are embarrassed and regretful that an intrusion was allowed to take place on our watch.

Please rest assured that no financial information whatsoever has been compromised. **While we are not aware of what data has actually been accessed or copied, the database included user e-mail addresses and other data you may have saved to your profile, such as your first name.** We are not aware of any files being accessed without permission, but we recommend that you change your account password and the passwords on any private folders as a security precaution.

DivShare's courage to communicate and [admit the security breach](#) at the first place, speak for a great deal of professionalism, since the short term negative impact of the breach is worth it compared to the long term negative publicity due to the fact that [a company acts like nothing ever happened](#) .

With DivShare still unaware of the severity of the breach and what type of data was accessed besides the email addresses and the associated names, it's stolen databases like these who act as the

foundation for targeted malware attacks, spear phishing attempts, and last but not least, spam, since the email database will sooner or later find itself in the hands of spammers.

Secunia: popular security suites failing to block exploits | ZDNet

In a recently [conducted comparative review](#) , Danish security company Secunia, tested the detection rate of 12 different Internet Security Suites against 300 exploits (144 malicious files and 156 malicious web pages) affecting popular end user applications, to find that even [the top performer in the test is in fact performing poorly in general](#) . Their conclusion :

"These results clearly show that the major security vendors do not focus on vulnerabilities. Instead, they have a much more traditional approach, which leaves their customers exposed to new malware exploiting vulnerabilities.

While we did expect a fairly poor performance in this field, we were quite surprised to learn that this area is more or less completely ignored by most security vendors. Some of the vendors have taken other measures to try to combat this problem. One is Kaspersky who has implemented a feature very similar to the Secunia PSI, which can scan a computer for installed programs and notify the user about missing security updates. BitDefender also offers a similar system, albeit this is more limited in scope than the one offered by Kaspersky and Secunia. We do, however, still consider it to be the responsibility of the security vendors to be able to identify threats exploiting vulnerabilities, since this is the only way the end user can learn about where, when, and how they are attacked when surfing the Internet."

And while it's boring to scroll through the empty tables of the study, is Secunia's report a frontal attack against the security software vendors' inability to block exploits, or are they trying to emphasize on the fact that the end user should make better informed purchasing decisions when relying on All-in-One Security products?

In 2007, Secunia released data indicating that [28% of all installed apps are insecure](#) , and despite that the vulnerabilities has been already addressed, the end users were still living in the reactive

response world. Cybercriminals on the other hand, took notice, and following either common sense or publicly obtainable data indicating that end users remain susceptible to already patched vulnerabilities, started integrating outdated exploits into what's to become one of the main growth factors for web malware in the face of today's ubiquitous [web malware exploitation kits](#) .

A year later, [another study confirmed this fact](#) and pointed out that one of most effective vehicle for the success of web malware -- the insecure web browser -- remains largely ignored by millions of Google users. So, theoretically, the more traffic the malicious attackers acquire and redirect to their exploit serving domains, the higher the probability for a successful infection with an undetected by standard signatures based scanning piece of malware - which is exactly what they've been doing the entire 2007 and 2008.

What is more important, to detect the latest malware binary behind the exploit serving file, or prevent the latest malware binary from reaching the end user/company by blocking the relatively static exploit serving file? It's all a matter of perspective.

Naturally, the reactions to [the comparative review](#) , and the methodology used are already receiving criticism from the vendors. [Sunbelt Software's Alex Eckelberry comments on the report](#) , and also includes [AV-Test.org's](#) Andreas Marx opinion emphasizing on why it's important to prioritize :

"In most cases, it is simply not practical to scan all data files for possible exploits, as it would slow-down the scan speed dramatically. Instead of this, most companies focus on some widely used file-based exploits (like the ANI exploits) and some companies also remove the detection of such exploits after some time has passed by (as most users should have patched their systems in the meantime and in order to avoid more slow-downs). There are a lot more practical solutions built-in to security suites, like the URL filter (which checks and blocks known URLs which are hosting malware or phishing websites) and the exploit filter in the browser (which would also block access to many "bad" websites). Some tools also have virtualization and buffer/stack/heap overflow protection mechanisms included, too.

Then we have the traditional "scanner" -- and even if some exploit code gets executed, a HIPS, IDS or personal firewall system might be able to block the attack. For example, some security suites are knowing that Word, Excel or WinAmp won't write EXE files to disk -- so potentially dropped malware cannot get executed and the system is left in a "good" state."

Emphasizing on defense-in-depth, and prioritizing in the case of blocking the most popular exploits used is a very good point since it has the potential to protect as many customers as possible from the default set of exploits used in the majority of malware attacks. For instance, [the massive SQL injections attacks](#) that took place during the last couple of months, were all relying on [relatively static javascript file](#) , whose generic detection is a good example of prioritizing. Moreover, due to the evident [template-ization of malware serving sites](#) , and the commoditization of web malware exploitation kits, the impact of ensuring that your customers are protected from the default sets of exploits included within these kits, means that your customers will be protected from a huge percentage of web based malware attacks.

No Internet Security Suite [can protect you from](#) yourself, [so do yourself](#) and the Internet a favor - [patch all your insecure applications](#) - it's free.

Secunia: Average insecure program per PC rate remains high | ZDNet

With the time frame for an exploit to become an inseparable [part of a web malware exploitation kit](#) shrinking, and with the average Internet user's over-confidence in an antivirus scanner's ability to detect and block exploits ([Secunia: popular security suites failing to block exploits](#)) it shouldn't come as a surprise that Secunia's recently released WorldMap shows a relatively high rate for insecure programs found on a single PC.

The [WorldMap of patched and unpatched PCs](#) is released prior to an updated version of Secunia's [Personal Software Inspector](#) , with the latest version finally filling a niche left open potentially undermining the usefulness of the handy tool in general - [measuring the exploitability of cross-browser plugins](#) such as Adobe Flash Player, QuickTime, or Sun's Java.

Let's take a look at some of their stats.

North America is led by Cuba with 15 insecure programs on average, and with 4 insecure programs on average, Canada and Mexico lead [the U.S which has 3 insecure applications installed per PC](#) . However, Secunia's emphasis on the big picture points out that there are at least [2.7 billion vulnerable programs installed in the U.S alone](#) .

[Mikkel Winther comments](#) :

The fact that US based PC users have more than 2.7 billion vulnerable programs installed are shocking! And quite frankly I am very surprised, we had an idea it would be bad, but couldn't imagine the enormous scope of this problem. And to make things even worse, the picture formed in the US is the same all over the world. PC users need to patch! They need to patch all their vulnerable programs and they need to do so as fast as possible after the patch has been issued from the vendor. Failing to do so is playing Russian Roulette with your IT security – it is only a question about time – and luck – when your system will be compromised.

South America is led by Guadeloupe with [12 insecure programs in average](#) , San Marino with its [11 insecure programs on average](#) leads Europe, and Yemen with [12 insecure programs on average](#) tops Asia's chart. These results should be considered as very conservative, with the real data itself much more disturbing if only all the Internet users in these countries were running the PSI.

Despite the fact that according to Secunia's WorldMap there are countries like Burkina Faso with 20 insecure programs per PC, or Cuba with 15, it only takes a single unpatched application or a browser plugin in order for the cybercriminal to successfully exploit the host on-the-fly through a mix of popular exploits ([Cybercriminals release Christmas themed web malware exploitation kit](#)) embedded within a particular kit.

Prior to the official announcement of PSI 1.5, [Secunia stated that](#) *"patching is more important than having an Anti-Virus program and a personal firewall. "*

What do you think? Talkback.

Scareware scammers hijack Twitter trending topics | ZDNet

Researchers from [F-Secure](#) and [Sophos](#) are reporting on an ongoing scareware serving campaign abusing the popular micro-blogging service Twitter.

Hundreds of tweets using four different URL shortening services are currently spammed through the automatically registered Twitter accounts, relying on a pseudo-random text generation using Twitter's trending topics.

This isn't the first time ([Cybercriminals hijack Twitter trending topics to serve malware](#)) scareware scammers abuse Twitter, and definitely not the last. However, how are the scammers capable of achieving this automation ([Commercial Twitter spamming tool hits the market](#)), with Twitter now relying on [reCAPTCHA](#) for account registration purposes, a practice which is supposed to limit the automatic abuse of the service?

Pretty simple and that's the problem - the [underground going rate for a thousand solved CAPTCHAs](#) remains between \$1 and \$2, with [humans instead of bots doing the CAPTCHA recognition job](#).

This outsourcing approach is in fact so successful, that the companies offering these services now offer API keys to commercial spamming vendors that were once on the verge of irrelevance due to the mass adoption of CAPTCHA authentication, which they were unable to automatically recognize.

Go through related posts: [The ultimate guide to scareware protection](#) ; [Does Twitter's malware link filter really work?](#) ; [Commercial Twitter spamming tool hits the market](#) ; [Cybercriminals hijack Twitter trending topics to serve malware](#) ; [French hacker gains access to Twitter's admin panel](#) ; [Spammers harvesting emails from Twitter - in real time](#) ; [Twitter hit by multiple variants of XSS worm](#) ; [Koobface worm joins the Twittersphere](#)

Using such automatic account registration tools, the scammers behind the ongoing scareware-serving campaign at Twitter are

already reaching on average of 60 tweets per bogus accounts, with [the scareware](#) itself currently detected by only 2 out of 41 anti virus vendors.

Deeper analysis of the campaign reveals a connection to a well-known Ukrainian cybercrime enterprise that was also responsible for the recent [malvertising attack at the New York Times](#) , as well as the [Bahama botnet facilitating click-fraud](#) uncovered by ClickForensics.

Scareware pops-up at FoxNews | ZDNet

There [have been](#) numerous [reports](#) from [affected](#) users that a [scareware](#) variant of [PersonalAntivirus](#) and ExtraAntivirus has been popping-up at **FoxNews.com** during the last couple of days, through a malvertising campaign.

This most recent case of malvertising ([MSN Norway serving Flash exploits through malvertising](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#)) once demonstrates that whenever a direct access to a high-trafficked site cannot be obtained through a compromise, cybercriminals are logically exploiting third-party content/ad networks to achieve their goals.

Reproducing [malvertising campaigns](#) is tricky due to the geolocated nature in which the ads are served, as well as the cybercriminals' awareness on the fact that the amount of traffic which they expose to scareware is logically increasing the risk of having their campaign exposed. A risk which they hedge by temporarily inactivating the campaign or basically rotating the geolocation preferences and displaying the malicious ads to random countries.

Interestingly, in FoxNews.com's case [Google's Safe Browsing](#) diagnostic page is stating that "*Malicious software is hosted on 3 domain(s), including 2mdn.net/, s3.wordpress.com/, llnwd.net* " with **2mdn.net** part of DoubleClick's network, with another [interesting note](#) stating that "*Yes, this site has hosted malicious software over the past 90 days. It infected 18 domain(s)* ", confirmed by [another report](#) as well. These isolated incidents in the sense that the campaign's lifecycle is shortened based on collective reporting of affected users, are also taking place at other ad networks such as [ContextWeb](#) , and [Yieldmanager.com](#) .

Go through related rogue security software posts: [Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"](#); [Rogue security software spoofs ZDNet Reviews](#) ; [Sony PlayStation's site SQL injected, redirecting to rogue security software](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Google sponsored links spreading \(scareware\) rogue AV](#)

Here's a brief analysis of the campaign which now appears to have been removed by FoxNews. Until the next time. According to [SandShark](#) , the warning issued by Google's Safe Browsing was in respect to the a domain redirector **rd-point .net** which is still active and is redirecting to the rogue [ExtraAntivirus](#) (**extrantivirus .com**) followed by previous known redirectors to another scareware **RapidAntivirus** .

It's worth pointing out that a scareware pop-up at a high-trafficked web site that is basically relying on the social engineering factor, is not as ugly as the introduction of a [hybrid scareware demanding ransom](#) for the decryption of files, or [client-side exploits](#) . With the list of the major web properties that have been historically affected by much more malicious malvertising incidents (e.g. [MySpace](#) , [Excite](#) , [Expedia](#) , [Rhapsody](#)) continuously expanding, maintaining a decent situational awareness next to [a client-side vulnerabilities free host](#) , mitigates a great percentage of the currently active threats.

Who's to blame anyway - the advertising networks for working with phony content publishers, the affected web sites for not policing themselves, or the web site visitor for the lack of situational awareness on emerging threats/scams like scareware?

Talkback!

Scareware meets ransomware: "Buy our fake product and we'll decrypt the files" | ZDNet

A newly pushed scareware called [File Fix Professional 2009](#) (FileFix Pro 2009), has the potential to influence the way in which spreaders of rogue security software optimize their revenue in the future - by encrypting critical business files and requiring a \$50 purchase of the fake software for the decryption.

This piece of [hybrid ransomware](#) greatly reminds of June, [2008's GPCode targeted campaigns](#), where the malware author's tactic was undermined by their [inability to securely wipe out the deleted files](#), allowing their recovery without having to pay the authors.

Thankfully, [FileFix Pro 2009's encryption is anything but unbreakable](#), with several vendors already releasing free decryption tools. FileFix Pro 2009 [attempts to encrypt files](#) with the following extensions upon executing it:

- doc, xls, ppt, pdf, jpg, jpeg, png, mp3, wma, mdb, pst, docx, docm, dotx, dotm, xlsx, xlsxm, xltx, xltm, xlsb, xlam, pptx, pptm, potx, potm, ppam, ppsx, ppsm

A logical question remains - why did they introduce the ransomware motive within a business model that's proven to be highly successful, earning cybercriminals thousands of dollars daily? The economy slowdown affecting their revenues, or plain simple profit optimization strategy? I'd go for the second, and in particular a rather logical move given all the media attention rogue security software started receiving.

From an emphasis on visual social engineering, and traffic acquisition tactics, the affiliate networks set the standards on the basis of which the participants in the network operate. If this tactic goes mainstream, the affiliate network that first implements this on a large scale will be capable of stealing market share from competing networks due to the improved payout rates thanks to the ransomware motive. So far, that doesn't seem to be the case.

Go through related rogue security software posts: [Rogue security software spoofs ZDNet Reviews](#) ; [Sony PlayStation's site SQL injected, redirecting to rogue security software](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Google sponsored links spreading \(scareware\) rogue AV](#)

[FireEye Labs](#) , [Symantec](#) , and [third](#) party [researchers](#) have already released free [decrypting tools](#) for FileFix Pro 2009, affected parties can take advantage of.

Scareware goes Green | ZDNet

Malicious pseudo-environmentalists have come up with a new social engineering tactic aiming to improve the profit margins of their fake antivirus software releases - by promising to donate \$2 from every purchase for saving the Amazonian green forests.

The new scareware template branded as "[Green-AV Premier Edition 3.0](#) " is pitched as the *"World's First Antivirus Which Cares About the Environment "* and goes for a hefty price of \$99.99, in comparison to other scareware brands whose [price tags vary](#) from \$49 to \$79.

Green-AV's mission statement reads:

"Fighting viruses, spyware, malware is not only a question of security. Spyware actually abuses your computer, overuses CPU speed, network bandwidth, makes your PC run slow. As a result you start consuming more power, working longer, think of replacing your PC with a new one which brings more unrecyclable wastes (many computer's parts contain toxic wastes).

This way Green AV actually cares about the environment. We thought that our application can guard not only your PC, but whole Earth - our home planet. So to show how much we care we decided to send \$2 from each product sale on saving green forests in Amazonia."

Despite the social engineering efforts on behalf of Green-AV's authors, the *Secure SLL Connection* padlock image indicates the bogus nature of their antivirus protection claims. They actually meant SSL connection.

Scammers phishing for sensitive iPhone data | ZDNet

iPhone users beware - an [ongoing phishing campaign](#) impersonating Apple.com, attempts to trick users into submitting [sensitive device information](#), with the scammers in a perfect position to use the data in a countless number of fraudulent variations.

Here are more details on the campaign, and why would phishers want access to such information.

The phishing campaign has been in circulation for over two weeks, and continues using the "*FREE 1 Year Warranty Extension Offer*" theme in emails coming with subjects such as "*IMPORTANT: Your FREE iPhone Warranty Extension for 1 Year!*", leading to domain using fast-flux hosting infrastructure - **www.apple.com.PHISHING.com/uk/iphone/warranty.htm**.

What's also worth pointing out is that the phishers require the user to submit their email at the first stage of the process, presumably saving themselves time in validating it, or in an attempt to contact the recipient in the long-term requesting more data.

What are the phishers after? The email of the user, the Serial number, IMEI (International Mobile Equipment Identity), the type of iPhone (ie. 3G / 3GS) and the capacity of the device (ie. 16GB / 32GB).

Why would a phisher want access to such data? Whereas some would point out that they're interested in the practice due to [the blocked IMEI numbers of stolen devices](#), which they can now change to ones that are not blacklisted, the long-term possibility of building inventories of such data to be re-sold to criminals looking for ways to bypass prepaid SIM restrictions, is a fully realistic one.

Consider going through related posts: [iHacked: jailbroken iPhones compromised, \\$5 ransom demanded](#); [Source code for ikee iPhone worm in the wild](#); [iPhone's anti-phishing protection offers inconsistent results](#); [Apple adds malware blocker in Snow Leopard](#); [Apple \(Snow Leopard\) malware blocker collecting cobwebs](#)

Over the [past year](#) , there have been [numerous developments](#) internationally aiming to [restrict the selling](#) of [prepaid SIM cards](#) , which offer a [safe heaven for criminals](#) since no personal identification is [required/stored](#) when [purchasing them](#) .

With safety measures varying from mobile carrier to mobile carrier, with only a few publicly disclosing the protections they've built in order to limit the use of cloned devices on their networks, [there are still countries where the lack of basic restrictions](#) is naturally resulting in demand for such data, which the cybercrime ecosystem can easily supply through phishing campaigns.

The entire business model can be undermined by the mobile carriers realizing the potential for abuse, and by those actually obliged by law to ensure such activities cannot take place within their networks.

Scammers introduce ATM skimmers with built-in SMS notification | ZDNet

The bust of the notorious [ATM scammer](#) going under the handle of [Cha0 in early September](#) , once again puts [ATM skimming](#) in the spotlight. Among the main insecurities scammers face while embedding an ATM skimmer, is the retrieval process of the device that is now containing the credit card details of several hundred people depending on the volume of transactions that occurred while the device was in place. How are then scammers going to minimize the risk of getting caught without having to come back at the crime scene? A recently uncovered serial manufacturer of ATM skimmer devices, seems to have solved the secure retrieval of the device issue by innovating, and introducing ATM skimmers that would automatically SMS the complete credit card details to the scammer.

How much does the device cost, how does it work, what ATM skimming tips is the manufacturer offering, and also, how can you protect yourself against ATM skimming? Let's find out.

Starting from \$8,500 and capable of sending 1,856 SMS messages -- processed credit card details -- without any charging the introduction of built-in SMS notification, and the ability to "call the ATM skimmer" in order to retrieve the information, is a major milestone for an ATM skimming device.

How does the device work according to the "manufacturer"?

"The card reader reads out cards and sends tracks via SMS. The keyboard tracks the pressed buttons sequences and also sends them via SMS. If it is necessary, you can make a call to skimmer and download information, but it's more convenient to receive SMS. All SMS are being sent to a basic number defined by a Client, a sim card with a basic number is installed into the phone (we tell you the cellular phone model when you buy the skimmer). The phone is connected to a PC with running a certain software that controls the device functioning. In other words, You receive tracks and PINs, manage your device just sitting at home in front of your PC. Then we

deciphering the data received. The data received by your PC is being coded instantly to prevent it being used and accessed by unwanted persons. To decipher the data one should use a special software that is supplied with the device. The data deciphered is ready for writing on cards. The equipment is designed for several ATM types that are widespread in Europe, USA, Australia and Arab states. The skimmers' model line allows you to work in any city worldwide."

It's worth pointing out that the security process of "coding the data" and deciphering the skimmer credit card details are built with the idea to ensure that the organizers of the credit card theft group are not going to get scammed by other people working for them :

"Thus, you receive and use absolutely safe software. Even if someone take a look at your PC's display when the software is running, it wouldn't help a bit, even if this is a person that can tell one track from some other info. So, you use the system one cannot steal tracks from. This means that all your workers wouldn't be able to steal tracks, you'll be the only one who can fully access the information captured. Why the GSM is used? The service is based on GSM standard because you can receive SMS anywhere, would it be your home or a sunny beach. It is the most solid security in our days. ... how many people were arrested only because they had used skimmers without data transfer... In return, no one has ever been arrested when using our skimmer. "

How are they capable of producing such legitimately looking ATM skimmers? They seem to be [using the very same manufacturer that the banks are using](#) , indicating possible cooperation with insiders or highlighting the insecure processes within manufacturers supplying anyone that pays with the ATM components :

"The skimmers form is being created on the basis of the pattern of the real ATM models. In other words, if the real ATM model has smooth lines, then our skimmers would be designed in accordance. That's why skimmer looks even like an integral part of an ATM. The body of all skimmers is colored with the same paint that ATM manufacturers use (we are buying paints at the same facility). We take exactly the same color and hue required by the model of the

real ATM. The technology of painting is the same, we reproduce all the necessary characteristics like the temperature, the angle of paint drop, the pressure, polymerization time etc. Thus, we achieved the full and precise compliance of the paint's tone, gleam, hue at the different light angles, the paint's surface feelings to the touch etc. In the real situations the skimmers really look like an integral part of ATM."

How does the device work, and how many SMS messages is it capable of sending without recharging the battery?

"Our skimmers read out the magnetic strip in two ways, there and back. The skimmer reads off the streap in both ways if there is 2 tracks. The skimmers reads off the strip even if there is only 2 tracks on the strip (that happens with electrons'). The data can be read off even if a holder passes the card changing speed or with a jerk. The skimmers fail-safely reads off data: 9,999 tries of 10,000 are successful. It works even if a holder passes the card fast and then slow it down. The only situation when the skimmers fails is when the card is stopped in the middle while being passed. It's a typical error for all card reading devices linked to the magnetic stripes read off technology.

All devices are powered with Li-on batteries. The charger is delivered with devices. The battery can works fully 24 hours (when the temperature is 21 degrees centigrade). We conducted the test on the maximum number of SMS sent using one battery. **The result is really great: 1,856 SMS were sent without any charging.** The tester were passing a card permanently without any pauses from 03 a.m. to 5 p.m. Usually during a day the number of holders is less than 1,856 and the Skimmers is in the waiting mode, consuming less energy. So, in the normal mode one battery can work 24 hours."

The manufacturer seems to be a group of experienced ATM skimmers that have applied a great deal of security measures in order to ensure that their customers don't get caught while retrieving the data. For instance, in one of the cases they seem to have been observing how would the police react upon detecting the skimmer, and "just like they thought" while they were patiently waiting for

someone to retrieve the device and bust him, the skimmed data has already been SMS-ed.

Interestingly, not every average credit card thief will be able to purchase the device unless he has recommendations and is a known "usual suspect" :

"But we do not sell to anyone and anytime. To buy the skimmers you should have recommendations, only in that case we can talk about the deal. We do not sell the equipment in stock anytime because we do not have the assembled equipment. Sometime we assemble few suites and sell them, but we do not always have assembled suites in stock. That's why when we offer you're the equipment here and now, you'd better buy it immediately because, say, in a week we wouldn't have them in stock. "

How much does the device go for? Depends on the ATMs it's capable of fitting into and the number of skimmers the buyer requests :

"All models have the same price. 1 set = \$8.500 + shipment costs
2 sets = \$16.000 + free shipment 3 sets = \$24.000 + free shipment 4 sets = \$32.000 + free shipment 5 sets = \$40.000 + free shipment
The price for two-model set is \$9,800

We always quickly ship orders. We ship orders worldwide. I don't like unresolved questions that's why it pays to deliver the order ASAP as we receive the money. The faster we send the better we sleep. That's why we talk about selling only assembled and ready-to-go devices. In other words, you wouldn't wait ages while your equipment is being assembled, tested etc. We sell only tested equipment.

How we do tests? 1. Every devices are tested for bugs during 24 hours marginally. 2. Every shell is trying on the native model to ensure ideal installation 3. Every shell is thoroughly checked for painting defects etc, the client receives defects free equipment Shipment methods, terms and details are defined individually. We conduct shipment of every order using different methods, from different cities and countries for the security matters."

Just like Ebay's feedback system aiming to build trust among sellers and buyers, the underground ecosystem has been unofficially maintaining lists of scammers within the scammers, with sales of a particular service or product driven mainly because of the positive or negative feedback. In regard to this particular ATM skimmer, the scammers that have already purchased it are all giving positive feedback. Would the built-in SMS notification within an ATM skimmer render news items like "*Police Release Photo of ATM 'Skimming' Suspect*" pointless? If they start standardizing the feature, that could well be the case, for the time being, it once again proves that mandatory prepaid card registration could come handy in solving these, and many other crime cases.

Who's to blame at the bottom line, the bank or the shopping center maintaining the ATM for not physically inspecting it on a daily basis, the component manufacturers for having obvious loopholes within their security processes, or the end user for not having a decent situational awareness about how to protect himself? [It's a shared responsibility](#) , but going through [Cha0's tips for committing ATM fraud](#) might come handy from the perspective of knowing how an ATM skimmer thinks before the device is installed.

Scammers caught backdooring chip and PIN terminals | ZDNet

The U.K's [Dedicated Cheque and Plastic Crime Unit \(DCPU\)](#) have recently uncovered state of the art social engineering

scheme, where once backdoored, chip and PIN terminals were installed at retailers and petrol stations in an attempt to steal the credit card details passing through. Originally, before online banking took place proportionally with the developments on the banker malware front, scammers used to take advantage of old-fashioned ATM skimming and fake keypad devices, which were installed at less popular locations due to the possibility of them getting caught. What this case demonstrates is that even trustworthy locations where you'd assume that a physical breach cannot take place that easily, remain vulnerable.

"According to police the tampered chip and PIN terminals are installed in (30) retail outlets and petrol stations either by someone working on the inside or by threatening staff. The criminals are then able to steal card details and PIN numbers. These are then used to create fake magnetic stripe cards containing the stolen card details, which can be used to withdraw money from cash machines or pay for goods in shops in countries that have yet to roll out chip and PIN technology. "

And while details on how did manage to install them at the popular locations without getting noticed, and whether or not there were insiders involved in the scheme remain unclear, a similar incident which recently took place in Ireland may be directly related to this one. Basically, the scammers [installed the backdoored terminals by pretending to be bank technicians](#) , the rest is fraudulent history :

"Opportunistic data thieves — masquerading as bank technicians — have fooled shop owners into giving them access to credit card terminals and managed to download the details of over 20,000 credit and debit cards, it emerged this morning. The Irish Payment Services Organisation has warned that individuals pretending to be

from Irish banks convinced shop owners they were carrying out maintenance on behalf of banks. This enabled them to plug in wireless devices that pushed the data to the internet and allowed the card numbers to be used overseas."

From technical perspective, what these data thieves did is not rocket science, it's the direct result of a situation known as "when the academic community is talking nobody is listening until criminals do their homework". For instance, the folks working for the Computer Laboratory Security Group at the University of Cambridge have been extensively researching the trivial opportunities a criminal can take advantage of on his way to backdoor and tamper with chip and PIN terminals. What they're trying to achieve is raise more awareness on the fact that just because a financial institution has a Security Tips section on its web site, urging its customers to update their antivirus software, run a firewall and don't open phishing emails, shouldn't mean that the institution shouldn't be held liable for fraudulent transactions given the highly insecure equipment it's using at the first place. Here's some of their research worth going through :

[Chip & PIN \(EMV\) relay attacks](#) [PIN Entry Device \(PED\) vulnerabilities](#) [Chip & PIN \(EMV\) interceptor](#) [Tamper resistance of Chip & PIN \(EMV\) terminals](#)

[As far as online credit card fraud is concerned](#) , a recent survey that I did on the topic of whether or not stolen credit card

details are getting cheaper, not only revealed that it's all a matter from who you're buying them from, and how much you actually want to buy, but also, that [cybercriminals are using price discrimination based on the different banks and the account balances](#) when they last verified them. Today's availability of stolen credit card obtained through banking malware botnets is getting so prevalent, that what used to be [proprietary services offering access to such a botnet](#) allowing the buyer to sniff as many credit cards and login details as he wants to for a certain period of time, are going mainstream with cybercriminals wanting to sacrifice anonymity for the sake of reaching a wider audience.

What happens once the preferred tactic of choice takes place, and the credit card details get stolen through banker malware infected

hosts? Over at ISS's Frequency X blog, [Gunter Ollmann has been researching](#) the availability of tools and equipment allowing cybercriminals to quickly transform the [digital data they've obtained into real credit cards](#) , and the data speaks for itself.

[Never play Tetris on a backdoored terminal](#) , and stay informed.

SCADA systems at the Water utilities in Illinois, Houston, hacked | ZDNet

UPDATE: [DHS denies report of water utility hack](#)

According to reports, the SCADA systems at the Water utilities in Illinois, Houston were recently hacked by a malicious attacker using the handle "pr0f".

The attacker has posted evident proof of a [direct compromise of the SCADA system](#)s at this water utility, with a separate report confirming that there was actual damage - "[the SCADA system was powered on and off, burning out a water pump.](#)"

[More details:](#)

Joe Weiss, a managing partner for Applied Control Solutions, said the breach was most likely performed after the attackers hacked into the maker of the supervisory control and data acquisition software used by the utility and stole user names and passwords belonging to the manufacturer's customers. The unknown attackers used IP addresses that originated in Russia.

[More details from Weiss :](#)

The disclosure was made by a state organization, but has not been disclosed by the Water ISAC, the DHS Daily unclassified report, the ICS-CERT, etc. Consequently, none of the water utilities I have spoken to were aware of it.

It is believed the SCADA software vendor was hacked and customer usernames and passwords stolen.

The IP address of the attacker was traced back to Russia.

It is unknown if other water system SCADA users have been attacked.

Like Maroochy, minor glitches were observed in remote access to the SCADA system for 2-3 months before it was identified as a cyber attack.

There was damage – the SCADA system was powered on and off, burning out a water pump.

Meanwhile, the "DHS and the FBI are gathering facts surrounding the report of a water pump failure in Springfield, Ill," [Boogaard wrote.](#)

Go through related posts:

[Researcher releases details on 6 SCADA vulnerabilities](#)
[Researchers releases details on 34 SCADA vulnerabilities](#)

Rustock botnet's operations disrupted | ZDNet

UPDATE: Microsoft claims credit for [disrupting Rustock's operations](#).

According to [Symantec](#) and [M86 Security](#), an unknown team of researchers managed to successfully disrupt the spamming operations of one of the most prolific spam botnets - Rustock. As of 15:30 UTC, on 16 March, none of its command and control servers were responding, resulting in the immediate [decline of spam originating from the botnet](#).

SecureWorks [Joe Stewart comments](#) :

“This looks like a widespread campaign to have either these [Internet addresses] null-routed or the abuse contacts at various ISPs have shut them down uniformly,” Stewart said. “It looks to me like someone has gone and methodically tracked these [addresses] and had them taken out one way or another.”

Is this a permanent disruption or a temporary glitch? According to Symantec, the botnet has gone quiet before when it stopped spamming for several days, but returned as strong as ever, with M86 Security speculating that it's too early to say goodbye to [the botnet](#).

Russian Embassy in London hit by a DDoS attack | ZDNet

The Russian embassy in London was hit by a distributed denial of service attack (DDoS) over the weekend. According to a [Tweet posted by the Embassy](#):

Our website is likely to have been brought down by a DDoS attack. But its mirror <http://www.rusemborguk.ru/> is up and running.

The attack was later on confirmed by a [press release issued by the Embassy](#):

Between 9 and 12 September 2011 the website of the Russian Embassy in London www.rusemb.org.uk repeatedly became unreachable. The nature of the disruptions, as well as our further communication with the hosting provider provided evidence of a DDoS attack against the server where the website is hosted. The Embassy responded by creating a “mirror” website www.rusemborguk.ru to satisfy the demand for information on the eve of PM David Cameron’s visit to Moscow. The website has since then been fully restored. The Embassy requested the British authorities to investigate the incident.

The attack came right before the Prime Minister David Cameron visit to Moscow, the first visit by a British leader to Moscow since the 2006 killing in London of a Kremlin critic.

The attacks appear to have been outsourced to a vendor of DDoS for hire services, and the political sentiment is pretty evident.

What do you think? Who was behind the DDoS attacks?

TalkBack.

RSA: Banking trojan uses social network as command and control server | ZDNet

RSA's FraudAction Research Lab is reporting that a [crimeware targeting Brazilian banks, is using a popular social network](#) as a command and control server.

According to the company, which acted promptly and took down the profile in question, cybercriminals continue to actively experiment with alternative C&C (command and control channels) using legitimate infrastructure.

More details:

The cybercriminal behind the crimeware set up a bogus profile under the name of "Ana Maria", and entered the crimeware's encrypted configuration settings as text uploaded to the profile.

After infecting a user's machine, and installing itself on it, the malware searched the profile for the string ELOWJE (underlined in the above screenshot). The string signified the starting point of the malware's configuration instructions.

All the encrypted commands following the ELOWJE string were decrypted by the malware and executed on the infected computer.

This isn't the first time that cybercriminals experiment with managed cloud platforms, or abuse of social networks for command and control purposes, and definitely not the last. Here are some example of known cases where legitimate infrastructure/social networks were used as C&Cs:

[Zeus crimeware using Amazon's EC2 as command and control server](#) [Twitter-based Botnet Command Channel](#) [Google Groups Trojan](#) [Trojan.Whitewell: What's your \(bot\) Facebook Status Today?](#) [The DIY Twitter Botnet Creator](#)

The same mentality was also applied in the ["Shadows in the Cloud" cyber espionage campaign](#), where the malicious attackers once again relied on legitimate infrastructure for command and control purposes:

The attackers also used Yahoo! Mail accounts as a command and control component in order to send new malicious binaries to compromised computers. In total, we found *three Twitter accounts, five Yahoo! Mail accounts, twelve Google Groups, eight Blogspot blogs, nine Baidu blogs, one Google Sites and sixteen blogs on blog.com* that we being used as part of the attacker's infrastructure.

Are social networks a heaven for cybercriminals and their botnets? Basically, they are. Social networks offer two of the most important things, a cybercriminal is seeking - potential for scalability where even the shortest time frame for a particular campaign would result in [hundreds of thousands of clicks](#), and the trust factor established by social networks.

Compared to [cybercrime-friendly ISPs](#), which remain the dominant hosting solution for cybercriminals, once detected, they are fairly easy to blacklist, even though some will remain online. However, this process gets undermined by the use of trusted social networks, and the main problem is that cybercriminals are perfectly aware of this fact.

Throughout the last couple of years, they started realizing that it's not just the clean network reputation that matters in a social networking environment, but the trusted reputation of the user at any particular social network. For instance, one of the most successful social networking malware, [the Koobface botnet](#) which gets the majority of its traffic from Facebook, doesn't rely on bogus user accounts to propagate. Instead, it hijacks the trusted reputation of everyone's friends on a large scale.

[RSA's assessment](#) concludes that malware using social networks is currently "*the exception rather than the rule*". What do you think? Is this the case, or are cybercriminals thinking "*the best is yet to come*" in the long term? What if today's fake account of Ana Maria, becomes tomorrow's legitimate account of Ana Maria, issuing commands to crimeware-infected hosts in a seemingly innocent fashion from a linguistic perspective?

Talkback.

Rogue security software spoofs ZDNet Reviews | ZDNet

Impersonation is a form of flattery by itself, however, not when it comes to the very latest round of rogue security software this time impersonating ZDNet, [CNET's](#) and [PC Magazine's](#) reviews section, making it look like legitimate and highly respected technology sites have actually reviewed and recommend the rogue security software.

According to Lawrence Abrams from Bleeping Computer the [latest rogue security software Anti-virus-1](#) redirects infected users attempting to visit the sites to a legitimately looking reviews of the scareware. By using this novel approach the rogue software vendor's aim is to add more legitimacy to Anti-virus-1's existence in general. However, if they truly wanted to achieve better social engineering result, they could have at least used a more recent version of the impersonated sites.

Here's how it's done anyway:

Upon installation the software modifies the HOSTS file and redirects affected users attempting to visit the review sites to a centralized location used for the hosting and promotion of even more rogue security software:

```
O1 - Hosts: 217.20.175.74 www.review.2009softwarereviews.com
O1 - Hosts: 217.20.175.74 review.2009softwarereviews.com O1 -
Hosts: 217.20.175.74 a1.review.zdnet.com O1 - Hosts:
217.20.175.74 www.d1.reviews.cnet.com O1 - Hosts:
217.20.175.74 www.reviews.toptenreviews.com O1 - Hosts:
217.20.175.74 reviews.toptenreviews.com O1 - Hosts:
217.20.175.74 www.reviews.download.com O1 - Hosts:
217.20.175.74 reviews.download.com O1 - Hosts: 217.20.175.74
www.reviews.pcadvisor.c.uk O1 - Hosts: 217.20.175.74
reviews.pcadvisor.co.uk O1 - Hosts: 217.20.175.74
www.reviews.pcmag.com O1 - Hosts: 217.20.175.74
reviews.pcmag.com O1 - Hosts: 217.20.175.74
www.reviews.pcpro.co.uk O1 - Hosts: 217.20.175.74
```

| | | | | |
|--------------------------------|----|---|--------|---------------|
| reviews.pcpro.co.uk | O1 | - | Hosts: | 217.20.175.74 |
| www.reviews.reevoo.com | O1 | - | Hosts: | 217.20.175.74 |
| reviews.reevoo.com | O1 | - | Hosts: | 217.20.175.74 |
| www.reviews.riverstreams.co.uk | O1 | - | Hosts: | 217.20.175.74 |
| reviews.riverstreams.co.uk | O1 | - | Hosts: | 217.20.175.74 |

www.reviews.techradar.com

And whereas modifying the HOSTS file is a bit of a noisy approach to hijack traffic, given the fact that end user managed to get -- ironically -- infected with a non-existent security software on their way to protect themselves from security threats, there's a high chance that this HOSTS modification will remain undetected.

Go through related rogue security software posts: [Sony PlayStation's site SQL injected, redirecting to rogue security software](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Google sponsored links spreading \(scareware\) rogue AV](#)

This "visual social engineering" approach is perhaps one of the key success factors for the rise of rogue security software. From the real-time scanning applets showing how badly affected a visitor is, to the bogus software rewards and awards the application has already won by using , vendors of rogue security software know the value of "what you see is what you get", or at least we want you think so.

From a psychological perspective, the rise of rogue security software demonstrates the end user's impulsive decision making based on the oldest known motivation factor - fear which in 2009 is transformed into fear of losing data. [And while in the past](#) cybercriminals [used to brandjack](#) legitimate [security software](#) , today's revenue-sharing affiliate based model for spreading rogue security software is in fact building new brands that despite their short product cycle are already affecting hundreds of thousands of users.

Rogue Firefox extension hijacks browser sessions | ZDNet

Security researchers from StopMalvertising, have spotted [a rogue Firefox extension](#), capable of hijacking browser sessions and posting content on Facebook.

The rogue extension is currently distributed across multiple adult web sites, and across Facebook, attempting to trick users into thinking that they're running an outdated version of their Adobe Flash Player.

What happens once the user installs the bogus extension?

The internet user will visit additional websites in the background with the viral add-on installed, possibly participate in click-fraud and expose themselves to malware while surfing on those unwanted sites. Furthermore, when logged in on Facebook, the victim will spam a viral video to their friends, spreading the Trojan clicker even more.

When visiting Google for example, the script will fetch additional web pages in the background which may lead to malware. The page at **footprintsit.com** contains a list of URL's to visit. The URL also contains an affiliate ID / Name ... Foreste. This is the criminal who will earn money from your surfing.

If the affected user is logged into Facebook, the rogue extension will distribute a viral video with the title "*Kristen Stewart Was Taped Drunk & Having S#x!*", in an attempt to trick even more people into downloading and installing the bogus extension. Affected Facebook users will be served a bogus Facebook landing page, prompting them to install **Flash_Player_11.exe**.

Users are advised to be extra cautious when installing Firefox extensions from untrusted sources, and to avoid falling victims into scams impersonating legitimate companies by always ensuring that they are downloading third-party software and browser plugins from their official sites only.

Ringleader of cybercrime group to be offered a job as cybercrime fighter | ZDNet

Owen Thor Walker, a 18 years old ringleader of an international cybercrime group, known as AKILL, part of the A-Team, a group of 8 script kiddies which were all caught in a operation called "[Operation Bot Roast II](#) " bust executed by the FBI and several international law enforcement agencies in 2007, responsible for pump'n'dump stock price manipulations through spam, infecting 1.3M computers with malware, further infecting them with spyware earning nearly \$40,000 in the process, in between launching a DDoS attack against the University of Pennsylvania, causing an overall damage of over \$20M, [has been discharged and could be offered a job as a cybercrime fighter](#) :

In court yesterday, Walker, who has Asperger's syndrome, a mild form of autism, smiled as he heard the prosecution describe how international investigators **considered his programming to be 'amongst the most advanced' they had encountered** . Judge Judith Potter described him as a young man with a bright future and ordered him to pay damages and costs of £5,500, but did not record a conviction. Detective Inspector Peter Devoy said that while **'there is no offer on the table, the option is being kept open'** . Maarten Kleintjes, head of the police e-crime laboratory, said the **self-taught Walker had a unique ability and was 'at the top of his field'** .

It's one thing to discharge him given his age, but entirely another to be publicly fascinated by what he did, state it publicly, and even consider the possibility of offering him a job, which indicates a great deal of ignorance from those who "ought to know".

He is neither a hacker, nor a computer genius possessing some kind of unique skills, he's just someone proving for yet another time that it's not a matter of lack of capabilities for committing cybercrime, but a matter of courage to so. [A little something on his "considered to be" highly sophisticated malware](#) :

"The bot code is considered very advanced by international cyber crime investigators, containing a number of sophisticated features that protect it from discovery, allow it to spread automatically and allow it to identify and destroy rival bot code. One feature automatically disabled any antivirus software on an infected computer and prevented the software from being updated, say the documents. "

In reality though, his malware bot going under the name of [AkBot](#) is using modules from commodity malware bots, namely

, what he did is combined different scanning modules attempting to locate hosts vulnerable to a different set of vulnerabilities, compared to the misunderstanding that he had coded the bot from scratch. Each of these features, next to the many others offered by an average malware bot freely available for download on the Internet, aren't exclusive, but commodity features. Moreover, given that today's malware bots are open source ones, what he did is modify the command and control locations, then compile and start spreading the bot.

The day when a script kiddie knowing how to compile their own botnets after watching a video tutorial that comes with the bot is called a hacker, or being offered a job for using a already available feature allowing the "killing of running security software" and preventing it from reaching its update locations by, is the day when you're officially admitting you have absolutely no idea what's going on online. Here's a sample output from a sandboxed copy of one of his malware variants scanning for MS04-012: DCOM RPC Overflow exploit and MS04-011: LSASS Overflow exploit at large :

```
"PRIVMSG #yahoo :[MAIN]: Status: Ready. Bot Uptime: 0d 0h 0m.
PRIVMSG #yahoo :[MAIN]: Bot ID: rx-asn-2-re-worked . PRIVMSG
#yahoo :[SCAN]: Exploit Statistics: Dcom135: 0, Dcom445: 0,
Dcom1025: 0, Isass_445: 0, Isass_139: 0, dcass: 0, MassAsn: 0,
plugnpay: 0, VNC: 0, netapi: 0, sym: 0, asn1http: 0, asn1smb: 0,
asn1smbnt: 0, Total: 0 in 0d 0h 0m. PRIVMSG #yahoo :[MAIN]:
Uptime: 0d 0h 2m. PRIVMSG #yahoo :[PROC]: Failed to terminate
process: PROCESS_NAME_TO_TERMINATE PRIVMSG #yahoo :
[HTTPD]: Server listening on IP: *.*.*:5678, Directory: \. PRIVMSG
```

```
#yahoo :[DDoS]: Done with flood (0KB/sec). PRIVMSG #yahoo :  
[DDoS]: Flooding: (*. *.*.*:1234) for 50 seconds. PRIVMSG #yahoo :  
[SYN]: Done with flood (0KB/sec). PRIVMSG #yahoo :[SYN]:  
Flooding: (*. *.*.*:1234) for 50 seconds. PRIVMSG #yahoo :[SCAN]:  
IP: *.*.* Port: 1234 is open. PRIVMSG #yahoo :[SCAN]: Port scan  
started: *.*.*:1234 with delay: 50(ms). PRIVMSG #yahoo :[UDP]:  
Sending 40 packets to: *.*.*. Packet size: 50, Delay: 60(ms).  
PRIVMSG #yahoo :[PING]: Finished sending pings to *.*.*.  
PRIVMSG #yahoo :[PING]: Sending 40 pings to *.*.*. packet size:  
50, timeout: 60(ms). PRIVMSG #yahoo :[UDP]: Finished sending  
packets to *.*.*."
```

This isn't ground breaking, it's in fact outdated and being impressed by this enough to even consider offering him a job could not just set an important precedent, but in fact question the expertise level of those impressed by his sophisticated malware bot.

If the size of the botnet matters, and speaks for some kind of pseudo-unique capability to utilize client-side vulnerabilities using publicly obtainable web malware exploitation kits, initiate an international "We are hiring!" campaign and have botnet masters replace cybercrime experts based on how much they impress you at the job interview, and, of course, based on what the RBN wrote about them in its recommendation based on their previous working relationship.

Researchers use smudge attack, identify Android passcodes 68 percent of the time | ZDNet

In a movie-plot like scenario, where a biometric system is bypassed using restored fingerprint samples, Penn State researchers managed to identify the pass code patterns on two Android smartphones (the HTC G1 and the HTC Nexus One), 68% of the time, using photographs taken under different lighting conditions, and camera positions.

From their paper, "[Smudge Attacks on Smartphone Touch Screens](#)":

To explore the feasibility of smudge attacks against the Android password pattern, our analysis begins by evaluating the conditions by which smudges can be photographically extracted from smartphone touch screen surfaces. We consider a variety of lighting angles and light sources as well as various camera angles with respect to the orientation of the phone.

Our results are extremely encouraging: in one experiment, **the pattern was partially identifiable in 92% and fully in 68% of the tested lighting and camera setups**. Even in our worst performing experiment, under less than ideal pattern entry conditions, the pattern can be partially extracted in 37% of the setups and fully in 14% of them.

The experimenting took place using two different scenarios - **the passive attacker**, who operates from a distance, and **the active attacker** who has breached the physical security of the device, namely, has physical access to it. Even in the worst possible experiment conditions, they were still able to partially extract 37% of the setups, and fully in 14% of the cases, using residual oils on the touch screens.

Related post:

[Man-in-the-middle attacks demoed on 4 smartphones](#)

The research recommends that "*Android's password pattern, should be strengthened*". From another perspective, entrusting the confidentiality of your data to a highly marketable, user-friendly touch screen password pattern, is a bad decision in the first place, if the user is not considering the use of third-party data encrypting applications in case the device gets stolen/lost.

Researchers spot scammers using fake browser plug-ins | ZDNet

Security researchers from Symantec, have spotted a [fake browser plugin-in](#) currently circulating in the wild.

How the infection takes place:

The scenario is very simple: the victim is lured into watching some video; but instead of asking the victim to share/like the video, (which we have seen in many scams) the scammers present the victim with a fake plug-in download image, which is required to see the video.

Once the end users are tricked into installing the fake YouTube themed browser extension, their User-Agent info is retrieved and accordingly, the fake plug-in is downloaded. For the time being, only Mozilla Firefox and Google Chrome plug-ins are being used.

The scam is currently circulating, using the ***[Video] Leakead video of Selena Gomez and Justin Beiber [NEW HOT!!]*** theme.

This isn't the first time that scammers are relying on fake browser plugins and extensions as a propagation vehicle for their scams. In December 2011, researchers from WebSense have detected a malicious campaign where the scammers were [successfully hijacking Facebook accounts using bogus browser extensions](#).

Facebook users are advised to be extra vigilant when interacting with content shared on the most popular social networking site.

Researchers spot pharmaceutical spam campaign using QR Codes | ZDNet

Spammers are no strangers to new technologies, and as true marketers, would do everything to achieve the objectives of their marketing campaign.

Security researchers from WebSense, have detected [a spam campaign using QR codes](#). Scanning the QR code with a QR reader will load the pharmaceutical spam URL in the browser.

More details:

The spam email messages look like traditional pharmaceutical spam emails (image 1) and contain a link to the Web site 2tag.nl. This is a legitimate Web service that allows users to create QR codes for URLs. Once the 2tag.nl URL from the mail message is loaded in the browser, a QR code is displayed, along with the full URL that the QR code resolves to on the right (image 2). When the QR code is read by a QR reader, it automatically loads the spam URL(or asks before loading, depending on which flavor of QR reader you have installed) (images 3 and 4).

This isn't the first time that cybercriminals use QR codes to spread scams and malicious content. In September, 2011, security researchers from Kaspersky Lab discovered a [malware campaign relying on QR codes](#) for spreading of mobile malware.

Researchers spot new Web malware exploitation kit | ZDNet

Over the past two years, the security industry witnessed the tremendous growth of web malware exploitation kit as efficient platforms for serving client-side exploits and malware to unaware end and corporate users.

The trend, largely driven by the professional work done on behalf of the cybercriminals behind these kits, is largely attributed to the standardized model behind the release of these kits. On a periodic basis, copycat cybercriminals will basically rebrand a well know web malware exploitation kit, introduce a new layout template, combined with a unique mix of exploits, and start advertising it within the cybercrime ecosystem.

On the other hand, sophisticated cybercriminals will do their best to stay beneath the radar of security researchers and security vendors, and will only serve a dedicated market segment within the underground economy.

This is exactly the type of web malware exploitation kit that [researchers from SpiderLabs recently spotted](#). Meet the RedKit, a private web malware exploitation kit, exploiting popular and already patched Java vulnerabilities, next to having an embedded QA (quality assurance) element embedded into it.

What's so special about RedKit, and how does it differentiate itself from the rest of the exploit kits currently observed in the wild? Next to exploiting [CVE-2010-0188](#) and [CVE-2012-0507](#), the cybercriminals behind the kit also offer legitimate traffic that will be later on converted to malware-infected hosts as a managed service.

See also:

[Web malware exploitation kits updated with new Java exploit](#)
[Which are the most commonly observed Web exploits in the wild?](#)
[Report: Patched vulnerabilities remain prime exploitation vector](#)
[Seven myths about zero day vulnerabilities debunked](#)

Moreover, in order to evade detection by security vendors, the cybercriminals behind the kit have introduced an API feature, helping customers of the kit acquire a new exploits-serving URL on an hourly basis. The next, and perhaps most important quality assurance element in the kit's propositions, is the fact that the malicious binary will be pre-scanned against 37 different antivirus vendors such as:

A-Squared, AVG8, AVL, ArvaVir, Avast, Avira, BitDefender, ClamWin, Comodo, DigitalPatrol, DrWeb, Emsisoft, Ewido, F-Prot, F-Secure, GData, IKARUS, IkarusT3, KAV8, McAfee, NOD32, Norman, OneCare, Panda, QuickHeal, Rising, SAV, Solo, Sophos, TrendMicro, TrendMicro2010, Vba32, Vexira, VirusBuster, Webroot, ZoneAlarm, eTrust

in order to ensure that the malicious binary has a low detection rate before serving it to unsuspecting end and corporate users.

Thanks to the fact that this is a private kit, not actively advertised across popular cybercrime-friendly web forums, it will never manage to gain the market share of publicly obtainable exploit kits such as the market leading BlackHole web malware exploitation kit.

Rather surprisingly, researchers from SpiderLabs, have already intercepted an increase in attacks using the RedKit, indicating that the invite-only business model seems to be working.

What happens once an exploit kit gains a high market share? Once an exploit kit becomes well known within the cybercrime ecosystem thanks to its high conversation rate -- traffic-to-malware-infected-hosts -- [international cybercriminals](#) will [localize these kits](#) to their [native languages](#), once again confirming that cybercriminals across borders are increasingly cooperating and working together.

Researchers spot new Mac OS X malware | ZDNet

[Security researchers from Sophos](#) have spotted a new piece of malware targeting Mac OS X users.

According to the company, the BlackHole RAT release is still under development, and appears to be using the source code of a popular Windows trojan horse known as darkComet.

The screen lock feature reads:

Hello I'm the BlackHole Remote Administration Tool. I'm a trojan horse, so I have infected your Mac Computer. I know, most people think that Macs can't be infected, but look, you ARE infected! I have full controll over your Computer and I can do everything I want, and you can do nothing to prevent it. So, Im a very new virus, under Development, so there will be much more functions when I'm finished. But for now, it's okay what I can do. To show you what I can do, I will reboot your Computer after you have clicked the Button right down.

Open source malware is an inseparable part of the cybercrime ecosystem, allowing novice cybercriminals to quickly catch up with that used to be sophisticated propagation tactics, a few years ago.

With open source malware now every day's reality, it shouldn't be surprising the the growth of malware is reaching such epic proportions of the overall picture. Although rate, malware releases for Mac OS X are only going to get more popular with the time, given the under served market segment, combined with the countless number of malware coders.

The company emphasizes the fact the BlackHole RAT isn't spreading in the wild, and urges users to exercise extra caution when downloading freeware applications, or even worse, pirated releases. A [short clip showing the trojan horse in action can be seen here.](#)

See also:

Malware Watch: Free Mac OS X screensavers bundled with spyware Mac OS X SMS ransomware - hype or real threat?

Researchers spot malware using a stolen government certificate | ZDNet

Researchers from F-Secure have spotted a [digitally signed malware using a stolen government certificate](#) belonging to the Malaysian Agricultural Research and Development Institute.

From F-Secure's post:

Every now and then we run into malware that has been signed with a code signing certificate. This is problematic, as an unsigned Windows application will produce a warning to the end user if he downloads it from the web — signed applications won't do this. Also some security systems might trust signed code more than unsigned code.

In some of these cases, the certificate has been created by the criminals just for the purpose for signing malware. In other cases they steal code signing certificates (and their passphrases) so they can sign code as someone else. We recently found a sample signed with a stolen certificate.

According to the vendor, the malware spreads through malicious PDF files that drop it after exploiting Adobe Reader 8. Interestingly, F-Secure notes that *"This particular malware does not gain much advantage of the signature any more, as the mardi.gov.my certificate expired in the end of September."*

The malware is currently detected as Trojan-Downloader:W32/Agent.DTIW.

Recommended reading:

[Google, Mozilla and Microsoft ban the DigiNotar Certificate Authority in their browsers](#) [The future of mobile malware - digitally signed by Symbian?](#)

Researchers spot fake mobile antivirus scanners on Google Play | ZDNet

Think that just because you're downloading an application from an official application store, you're safe from malicious software? Think twice.

Security researchers from AegisLab have spotted numerous [fake mobile antivirus scanners](#), currently available for download at Google's Play marketplace.

This isn't the first time that a fake mobile antivirus has been spotted in the wild, and definitely not the last. Last year, security researchers from CA spotted a [bogus Kaspersky-branded fake mobile antivirus application](#).

Users are advised to only download applications from known and trusted publishers, and to avoid secondary marketplaces as much as possible, and to also double-checked that they're downloading the official version of a particular application, not a bogus version of it.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Researchers spot a fake version of Temple Run on Android's Market | ZDNet

Security researchers from TrendMicro have spotted [a fake version of popular game Temple Run](#), currently available at Android's Market.

More details:

Once the application is installed and run, it creates shortcuts on an infected smartphone's homepage. If the Android-based device has Facebook installed, it asks the user to share the fake app on Facebook before playing the game. It would also prompt the user to rate the application in the Android Market. It also is capable of displaying ads using the mobile notification.

TrendMicro classified the application as malware due to the aggressive advertising methods used in it. It's currently detected as [ANDROIDOS_FAKERUN.A](#).

Researchers release details on 34 SCADA vulnerabilities | ZDNet

Security researcher [Luigi Auriemma](#) has released [proof of concept code for 34 vulnerabilities](#) affecting popular [SCADA systems](#). The majority of the vulnerabilities allow remote code execution on Internet connected systems, with the remaining offering access to stored data.

“SCADA is a critical field but nobody really cares about it,” [said the researcher](#). “That's also the reason why I have preferred to release these vulnerabilities under the full-disclosure philosophy.”

Affected products are:

- DATAAC RealWin 2.1 (Build 6.1.10.10) (SCADA)
- 7-Technologies IGSS 9.00.00.11059 (SCADA)
- GENESIS32 9.21(SCADA)
- GENESIS64 10.51 (SCADA)
- Siemens Tecnomatix FactoryLink 8.0.1.1473 (SCADA)

[*Image courtesy of Woodward*](#)

Researchers peek inside a mini Zeus botnet, find 60GB of stolen data | ZDNet

Just how much data can be harvested from 55,000+ crimeware-infected hosts?

According to a [newly published report](#) by AVG, upon obtaining access to a [mini Zeus botnet dubbed Mumba](#), part of [Avalanche group's](#) online operations, they found 60GB of stolen data such as, accounting details for social networking sites, banking accounts, credit card numbers and intercepted emails.

"Detected by AVG security products, the "Mumba" botnet was found to be using four different variations of the latest version of the Zeus malware to steal data from compromised machines. Zeus version 2.0.4.2 now supports the latest Microsoft operating system – Windows 7, and is able to steal HTTP traffic data from the Mozilla Firefox browser.

The "Mumba" botnet, which makes use of the prolific Zeus malware, has compromised more than 60GB of data from approximately 55,000 users' PCs around the world. The data includes user credentials of social networking Web sites, banking accounts, credit card numbers, email communications and more. "

Key points:

Windows XP Service Pack 3 users top the chart, followed by Service Pack 2 users

33 percent of the infected users are based in the U.S, followed by 17 percent based in Germany, and 7 percent in Spain

Over 60GB of stolen data from 55,000+ infected hosts found on a fast-fluxed infrastructure

Just like [the Kneber botnet](#), the Mumba botnet is a great example of currently ongoing experimenting on behalf of botnet masters in terms of partitioning their botnets in order to improve [operational security](#), and put contingency planning in place.

Having already anticipated the industry's improving capabilities of reverse engineering their command and control infrastructures, the bad guys are not just [diversifying their C&C channels through the use of legitimate infrastructure](#), but also, starting to realize that massive botnets are sitting ducks waiting to be reverse engineered to the point of shutting them down. Hence, the response with campaign-specific mini botnets using the DIY ZeuS crimeware kit.

Related posts:

[Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime](#) [Modern banker malware undermines two-factor authentication](#) [The Avalanche Botnet and the TROYAK-AS Connection](#)

This targeted approach allows them to collectively control botnet infrastructures which initially appear to be control by multiple gangs and botnet operators, all hiding under the umbrella of the ZeuS brand, or the brand of a particular web malware exploitation kit.

Meanwhile, AVG's findings perfectly fit the needs of the recently launched [Internet Fraud Alert Service](#), therefore communicating the stolen data through the intermediary, is crucial for timely reaching out to the infected uses.

For the time being, the DIY ZeuS crimeware kit, remains a key driving force for the growth of the cybercrime ecosystem, with the kit's success largely contributed to the use of [outdated security flaws](#) on a mass scale. If you want to learn more crimeware, how it works, how it matured from a DIY tool to a key growth factor in the Cybercrime-as-a-Service model, consider going through the [The current state of the crimeware threat](#) Q&A.

Researchers intercept Tatanga malware bypassing SMS based transaction authorization | ZDNet

Security researchers from Trusteer have intercepted a [Tatanga malware variant capable of bypassing the SMS based transaction authentication](#) protection of German banks.

Here's how it works:

The scam targets online banking customers of several German banks. When the victim logs on to the online banking application, Tatanga uses a MitB webinject that alleges the bank is performing a security check on their computer and ability to receive a Transaction Authorization Number (TAN) on their mobile device. In the background, Tatanga initiates a fraudulent money transfer to a mule account. It even checks the victim's account balance, and will transfer funds from the account with the highest balance if there is more than one to choose from.

The victim is asked to enter the SMS-delivered TAN they receive from the bank into the fake web form, as a way to complete this security process. By entering the TAN in the injected HTML page the victim is in fact approving the fraudulent transaction originated by Tatanga against their account.

What's particularly interesting about this Tatanga variant, is the fact that it doesn't attempt to undermine the technology of SMS based transaction authentication, instead it attempts to undermine the process. Next to undermining the technology, the malware will also attempt to hide the fraudulent activity from the eyes of the infected victim, by modifying the account balance reports.

Go through related posts:

[Modern banker malware undermines two-factor authentication Citizens Financial sued for insufficient E-Banking security. No security software, no E-banking fraud claims for you](#)

According to Trusteer, QA (quality assurance) wasn't applied in this sophisticated fraudulent attempt, since the message presented to the infected victim was full with grammar and spelling mistakes. As I've already discussed in previous posts, [localization on demand](#), a.k.a cultural diversity on demand is [available as a service within the cybercrime ecosystem](#), potentially allowing cybercriminals the option to have a well written and grammar and spelling mistakes-free message delivered do the prospective victims. It's very surprising that they didn't take advantage of such a service in this campaign.

[Two-factor authentication](#) has been under fire for years. [Today's modern crimeware variants](#), are fully capable of bypassing the multi-layered authentication process offered by financial institutions. What's even worse is that in 2012, novice cybercriminals can easily take advantage of [managed crimeware-as-a-service underground marker propositions](#), offering crimeware log files, or access to crimeware botnets.

Once you're infected with crimeware, it's game over. The solution? Try the concept of [using a Live CD for E-banking activities](#), or [USB sticks with write protect switch](#).

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

Researchers intercept targeted malware attack against Tibetan organizations | ZDNet

Security researchers from AlienVault Labs have [intercepted a currently circulating targeted malware attack](#) aimed at Tibetan activist organizations, including the Central Tibet Administration and International Campaign for Tibet.

More details:

The attacks begin with a simple spear phishing campaign that uses a contaminated Office file to exploit a known vulnerability in Microsoft. The information in the spear phishing email is related to the Kalachakra Initiation, a Tibetan religious festival that took place in early January. After further investigation, we discovered that the malware being used in this attack is a variant of Gh0st RAT (remote access Trojan), a type of software that enables anything from stealing documents to turning on a victim's computer microphone. Gh0st RAT was a primary tool used in the Nitro attacks last year and the variant we uncovered in these attacks seem to come from the same actors. It's likely that the same group is stealing from major industries as well as infiltrating organizations for political reasons.

The spear phishing emails contain a malicious file spamvertised as **Camp information at Bodhgaya.doc** , which upon execution attempts to exploit [CVE-2010-3333](#) .

What's particularly interesting about this targeted malware attack, is the fact that the malware is digitally signed, with the certificate issued to Qingdao Ruanmei Network Technology Co., Ltd.” by Verisign. Thankfully, the certificate has been revoked by VeriSign on 12th Dec.

Once a successful infection takes place, the malware phones back to the following command and control locations:

218.106.193.184 – China Unicom IP network
218.61.72.178 – China Unicom Liaoning province network
59.44.49.88 – CHINANET liaoning province network

With segmented databases of harvested emails for a particular country available for purchase within the cybercrime ecosystem, it shouldn't be surprising that the entry barriers in launching a targeted malware attack are constantly getting lower. Next to freely available RATs (Remote Access Trojans) the cybercriminals engaging in cyber espionage are also known to actively outsource their campaign needs to third-party providers of managed cybercrime-as-a-service market propositions.

With Tibet's current geopolitical position, the country is a common target for cyber espionage campaigns launched by Chinese hackers, thanks to the [China's government tolerance on homeland grown hacker communities](#), like for instance China's Blue Army.

Researchers find 12 zero day flaws, targeting 5 web malware exploitation kits | ZDNet

Security researchers from TEHTRI-Security, have found [twelve zero day flaws targeting five of the most common web malware exploitation kits](#) such as Neon, Eleonore, Liberty, Lucky and the Yes exploitation kits.

The use of these flaws could lead to hijacking of the admin panel, retrieving the admin password, or injecting content within the panel, potentially not just disrupting the campaign, but exposing the person behind it, or at least offering invaluable clues.

More details:

According to the group, some of the most widely used exploitation kits, are [susceptible to the following flaws:](#)

- Vuln in NEON Pack. Permanent XSS+XSRF.
- Vuln in NEON Pack. SQL Injection.
- Vuln in YES Pack. Remote File Disclosure.
- Vuln in YES Pack. Permanent XSS+XSRF admin.
- Vuln in YES Pack. Remote SQL Injection.
- Vuln in Lucky Sploit Pack. Remote control.
- Vuln in Liberty Pack. Permanent XSS+XSRF.
- Vuln in Liberty Pack. SQL Injection.
- Vuln in Eleonore Pack. Another SQL Inject.
- Vuln in Eleonore Pack. XSRF in admin panel.
- Vuln in Eleonore Pack. Permanent XSS.
- Vuln in Eleonore Pack. Remote SQL Inject.

These offensive tactics against cybercriminal are in fact nothing new. However, guess who pioneered the practice first? The cybercriminals themselves, allocating time and resources to finding remotely exploitable flaws within popular malware/web malware exploitation kits.

Related posts: [Pinch Vulnerable to Remotely Exploitable Flaw](#) ; [Help! Someone Hijacked my 100k+ Zeus Botnet!](#) ; [Firepack remote command execution exploit that leverages admin/ref.php](#) ; [The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw](#) ; [Cybercriminals release Christmas themed](#)

[web malware exploitation kit](#) ; [The Neosploit cybercrime group abandons its web malware exploitation kit](#)

Back in March, 2010, security researchers at the Vienna University of Technology, were able to easily extract 33GB of raw crimeware data, following a simple methodology - the lack of OPSEC (operational security) on the command and control servers responsible for maintaining the Zeus crimeware campaigns.

See: [The current state of the crimeware threat - Q&A](#)

And although they were surprised to find out how easily they could extract the data of the affected customers, they also admitted that it's fairly logical to assume that the cybercriminals are doing exactly the same against each other.

Last week, Microsoft in a cooperation with National Cyber Forensics Training Alliance (NCFTA), launched the [Internet Fraud Service Alert](#).

Basically, the service:

creates a trusted and effective mechanism for participating researchers to report stolen account credentials discovered online – such as username and password log-in information for online services or compromised credit card numbers – to the appropriate institution responsible for that account. Through a centralized alerting system powered by Microsoft technology developed specifically for this program, Internet Fraud Alert will quickly inform companies about compromised credentials, allowing them to take the appropriate action to protect their customers.

The current tactical advantage of the security community, is the fact that not all cybercriminals are willing to invest money into purchasing the latest exploitation kit/Zeus crimeware versions. Which, just as we see from the perspective of the legitimate user ([Does software piracy lead to higher malware infection rates?](#)), creates a lot of exploitation points.

The bottom line - in order for these offensive tactics against cybercriminals -- through the use of zero day flaws for instance -- to start producing actionable results which could drive the growth of the Internet Fraud Service Alert, the security community has to be a step

ahead of the cybercriminal attempting to exploit the vulnerable kit of another cybercriminal.

What do you think? Has to the time come to go offensive against cybercriminals on a large scale, by exploiting the very same exploitation kits that help them infect hundreds of thousands of people every day?

What should be the main emphasis of the practice? Tracking them down, or contributing to the growth of services such as the Internet Fraud Service Alert, leading to timely response to cybercrime incidents affecting the customers of the companies, participating in the project?

Talkback.

[Graph courtesy of BLADE's Evaluation Lab.](#)

Researchers expose complex cyber espionage network | ZDNet

Security researchers from the Information Warfare Monitor ([Citizen Lab and SecDev](#)) and the [ShadowServer Foundation](#), have released the findings from their eight month investigation, [“Shadows in the Cloud”](#), detailing the inner workings of complex cyber espionage network that was systematically stealing sensitive documents/correspondence from the Indian government, the United Nations, as well as Dalai Lama's offices, from January to November 2009.

More details on attack vectors used, the command and control infrastructure, and the victim analysis based on the recovered documents, some of which are marked as *SECRET*, *RESTRICTED* and *CONFIDENTIAL* :

Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Recovery and analysis of exfiltrated data, including one document that appears to be encrypted diplomatic correspondence, two documents marked “*SECRET*”, six as “*RESTRICTED*”, and five as “*CONFIDENTIAL*”. These documents are identified as belonging to the Indian government. However, we do not have direct evidence that they were stolen from Indian government computers and they may have been compromised as a result of being copied onto personal computers. The recovered documents also include 1,500 letters sent from the Dalai Lama's office between January and November 2009. The profile of documents recovered suggests that the attackers targeted specific systems and profiles of users.

Just like the majority of targeted malware attacks, this one was also relying on client-side exploits ([Report: Malicious PDF files comprised 80 percent of all exploits for 2009](#)) served through different file types (*PDF, PPT, DOC*) using a relevant topic of interest to Indian and Tibetan communities, which were then spamvertised to the victims of interest.

What's particularly interesting about the cyber espionage facilitating network in question, is the mix of legitimate and purely malicious infrastructure in an attempt to not only increase the life cycle of the campaign, but also, to make it harder for network administrators to detect the malicious use of popular free email service providers, as well as social networks.

[According to the report :](#)

During our investigation we found that such intermediaries included Twitter, Google Groups, Blogspot, Baidu Blogs, and blog.com. The attackers also used Yahoo! Mail accounts as a command and control component in order to send new malicious binaries to compromised computers. In total, we found three Twitter accounts, five Yahoo! Mail accounts, twelve Google Groups, eight Blogspot blogs, nine Baidu blogs, one Google Sites and sixteen blogs on blog.com that we being used as part of the attacker's infrastructure. The attackers simply created accounts on these services and used them as a mechanism to update compromised computers with new command and control server information.

The practice of blending [legitimate infrastructure](#) into the malicious mix is nothing new. In fact, in 2009 cybercriminals continued demonstrating their interest in abusing legitimate services such as [Twitter](#) , [Google Groups](#) , [Facebook as command and control servers](#) , as well as [Amazon's EC2 as a backend](#) .

Moreover, although the report is logically emphasizing on the actual attack vectors used in this particular cyber espionage network, there's another attack vector that's been trending over the past few years, having an identical cyber espionage potential to the targeted attacks in general.

The attack vector in question, is the client-side exploits serving embassy, with the following international embassies serving malware

to their visitors over the past few years as an example of the trend:

2007 - [Syrian Embassy in London Serving Malware](#) **2007** - [U.S Consulate in St. Petersburg Serving Malware](#) **2008** - [The Dutch Embassy in Moscow Serving Malware](#) **2008** - [Embassy of Brazil in India Compromised](#) **2009** - [Embassy of India in Spain Serving Malware](#) **2009** - [Ethiopian Embassy in Washington D.C Serving Malware](#) **2009** - [Embassy of Portugal in India Serving Malware](#) **2009** - [Azerbaijani Embassies in Pakistan and Hungary Serving Malware](#)

Who visits the web site of a particular embassy next to the people looking for information? It's the embassy staff itself, as well as other high-profile visitors. Therefore, a compromised web site of an embassy, which make in fact act as the weakest link in case it's insecure and open to exploitation compared to a failed targeted attack, could be on purposely used as an attack vector for a particular cyber espionage campaign.

The lines between cybercrime, and cyber espionage keep getting thinner, with financially-motivated cybercriminals today, in the best position to become information brokers of stolen high value data tomorrow, or even worse - set up the foundations for cyber espionage as a service propositions.

Google

disruptive.individuals@gmail.com

Zombie PC Prevention Bill to make security software mandatory | ZDNet

How do you fight botnets? With [rationalism](#), or with [radicalism](#)?

[South Korea's](#) recently proposed [Zombie PC Prevention Bill](#), aims to fight them with common sense - by making security software mandatory on users' PCs. What's particularly interesting about the bill, is the backdoor left open, empowering the government to "*examine the details of the business, records, documents and others*" of users and companies who do not comply.

More details on the bill:

- to impose a statutory duty on every citizen to install and to use security software pursuant to the Presidential Decree to be issued under the Act

- to confer on the government department (Korea Communications Commission; KCC) the power to ban or to allow the business of those security solution providers which KCC chooses to ban or to allow according to certain criteria

- to make the security solution providers to focus on winning the favor of government officials (through lobbying) rather than winning the consumers in the market through competition and innovation of product quality

- to empower the KCC agents, without a warrant, to "examine the details of the business, records, documents and others" of anyone upon mere suspicion that the person (individual or company) has violated the duty to use security software

In the past there have been numerous cases of enforced best practices, or how the lack of such may lead to unpleasant results:

- [End users without security software](#) cannot file fraud claims for their E-banking accounts

- [Commonwealth got fined \\$100k](#) for not mandating security software on its PCs

- [Citizens Financial got sued](#) for lack of sufficient E-banking security measures

What the MPs seem to have forgotten is the fact that antivirus software only mitigates a certain percentage of the risk, and is only part of a well developed defense in depth strategy. Multiple independent reports and tests show that despite that users are running antivirus software, they still get infected with malware.

What do you think is the best way to fight botnets? Rationalism or radicalism. Is running security software a duty, or has the time come for ISPs to take care of their own backyards.

TalkBack.

ZeuS crimeware variant targets Symbian and BlackBerry users | ZDNet

A ZeuS [crimeware variant](#) known as [ZeuS Mitmo](#) , has begun targeting the [two-factor authentication solution](#) offered by the Polish ING bank.

UPDATE: Devices running [Windows Mobile are also targeted](#) .

The variant, currently targeting Symbian and BlackBerry users works as follows. Upon successful infection, the crimeware injects a legitimately looking field into the web page. The aim is to trick end users into giving out their mTANs, which stands for mobile transaction authentication numbers. Now that the gang has obtained access to their cell phone number, including the type of the device, a SMS is sent back to the victim with a link to a mobile application targeting either Symbian or BlackBerry devices.

See also:

[Modern banker malware undermines two-factor authentication Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime](#)

According to the security researcher Piotr Konieczny, the reason why Apple's iPhone was excluded is due to the fact that Apple has more control over the Apple Store, compared to Symbian or RIM (Research in Motion).

These relatively [sophisticated attempts on behalf of cybercriminals](#) , wouldn't be possible to execute if the user didn't [get infected in the first place](#) .

As always, users are advised to use [least privilege accounts](#) , [browse the web](#) in [isolated environment](#) , and ensure their [hosts are free](#) of [outdated 3rd party software](#) , [browser plugins](#) or OS-specific flaws.

Zeus crimeware using Amazon's EC2 as command and control server | ZDNet

UPDATED: [ScanSafe posted an update](#) stating that *"In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008, and 22 in 2007. "*

Security researchers have intercepted a new variant of the [Zeus crimeware](#) , which is using [Amazon's EC2 services for command and control purposes of the botnet](#) . The cybercriminals appear to be using [Amazon's RDS](#) managed database [hosting service as a backend](#) alternative in case they loose access to the original domain, which would result in the complete loss of access to the compromised financial data obtained from the infected hosts.

Would 2010 be the year when crimeware will dive deep into the cloud, in an attempt to undermine the security industry's take down operations? With the [clear migration towards](#) the [abuse of legitimate infrastructure](#) we've observed throughout the entire 2009, this may well be the case.

Despite the fact that this is the first publicly reported case of Zeus crimeware ([Modern banker malware undermines two-factor authentication](#)) campaign abusing Amazon's cloud-based services, popular Web 2.0 services have also been under fire in recent months.

From the use of [Twitter](#) , to [Google Groups](#) and [Facebook as command and control servers](#) , these experiments clearly indicate that cybercriminals are cloud-aware, which isn't surprising given that from a distributed computing perspective, some of biggest botnets currently online can easily top the [Top 500 Supercomputing list](#) .

What exactly are they trying to achieve, and isn't the use of legitimate service for command and control purposes in fact a bad idea from a cybercriminal's perspective, compared to a situation where they'll be using the services of an ISP whose core

competency lies in ignoring abuse notification and cooperation with the security industry and law enforcement in general?

It's traffic camouflaging in the sense of making it harder to blacklist and detect potentially malicious activity hidden within the traffic stream between the infected host and a legitimate service.

'You've got a postcard' emails lead to exploits and scareware | ZDNet

Security researchers from WebSense have intercepted a [currently ongoing malware campaign](#), relying on spamvertised links to a bogus Greeting Postcard Service, the campaign aims to trick ends users into clicking on the link.

Upon clicking on the link, the users are exposed to client-side vulnerabilities which ultimately drop a [scareware variant](#).

Users are advised to [avoid interacting with suspicious links and email attachments](#) found in email messages.

'You visit illegal websites' FBI-themed emails lead to scareware | ZDNet

Multiple vendors are reporting on a currently ongoing spamvertised scareware-serving campaign, that's brand-jacking the FBI. The marked with "High Priority" emails attempt to impersonate the Federal Bureau of Investigation.

Sample subject: *You visit illegal websites*

Sample message: *Sir/Madam, we have logged your IP-address on more than 40 illegal Websites. Important: Please answer our questions! The list of questions are attached. pbu bx ng*

Sample attachment: *document.zip*

Upon execution document.exe drops a copy of the XP Total Security scareware, and is currently detected as Trojan.Zlob.2.Gen

Users are advised to avoid interacting with suspicious links and email attachments found in email messages.

Yahoo! Mail introduces two factor authentication | ZDNet

In an attempt to offer layered security to its millions of Web users, Yahoo Inc. recently announced the availability of [two factor authentication for Yahoo! Mail users.](#)

More on the feature:

Once the feature is turned on, any suspicious account sign-in attempt will be challenged by a second sign-in verification beyond the initial password validation. To confirm the legitimacy of the sign-in attempt, you or the hijacker will have to answer your account security question or enter a verification code that will be sent to your mobile phone. Presumably, only you, as the legitimate user, can sign in. Account hijackers will be blocked since they neither know your security answer nor possess your mobile phone.

Users who wish to active the [second sign-in verification](#) can do it through the Yahoo! Account Info page. The feature is currently available to users residing in the United States, Canada, India, and the Philippines, with the feature extending gradually to all worldwide users by March 2012.

Related posts:

[Survey: 60 percent of users use the same password across more than one of their online accounts](#) [Study: password resetting 'security questions' easily guessed](#) [Hotmail's new security features vs Gmail's old security features](#)

[Google announced the availability of two factor authentication](#) for Gmail users in February, 2011.

XSS worm at Justin.tv infects 2,525 profiles | ZDNet

A XSS worm was crawling across [Justin.tv](#) , the popular lifecasting platform at the end of June, details of the incident

emerged in the middle of last week. Basically, the group that found the XSS vulnerability abused it for the purpose of generating the following graph as a proof of concept, until Justin.tv fixed the flaw rendering the worm's activities obsolete. Now, [proof of concept of what exactly](#) remains questionable, since [if the research community was to exploit](#) every site [vulnerable to SQL injections](#) or [high profile sites vulnerable to critical XSS flaws](#) , in order to embedd a counter within and then come up with fancy graphs saying this is the number of people that could have been affected by this flaw, we would be dealing with more PoCs next to the real security incidents executed by malicious parties. This is the [statement made by one of the group members that released the PoC](#) :

"As of 'Sat, 28 Jun 2008 21:52:33 GMT' - An XSS worm was released on this website, this was and is meant only for research purposes. It was successfully executed and lasted roughly around 24 hours.

We have recorded such records making it possible for us to create graphical images graphing the progress of this XSS worm as it infected each profile upon the last being viewed. The XSS Vulnerability was discovered and fixed during 'Sun, 29 Jun 2008 21:12:21 GMT', with an after mass of 2525 profiles.

This actually is the very first XSS worm which we have unleashed, and it was solely upon research reasons; non-malicious at all :)

We've contacted the JTV Programmers prior to the fixing of the XSS worm and have sorted things out with them and made sure that they knew NO information such as IP Address, Cookies, Sessions and further information which poses private is not to be released. After that I put myself forward and found another XSS in turn to

prove that I was dedicated to helping JTV out in any further possible vulnerabilities", says x2Fusion. "

[Justin.tv fixed it shortly](#) after users started complaining :

"On Saturday we started to receive emails from users saying that their account had been compromised. On Saturday night we found a vulnerability that allowed someone to gain access to another users account without needing their username and password. Emmett worked tirelessly to fix the bug and released a patch on sunday morning. We were informed that as a result of the first vulnerability, personal communications from a number of justin.tv users were posted on flickr for all to see. We greatly regret that this occurred and apologize that we were not able to find and fix this vulnerability sooner. On tuesday and similar vulnerability was found and it was fixed within 2 hours."

The majority of social networking sites have all be subject to the efficient exploitation of a single XSS flaw, leading hundreds of thousands, sometimes millions of users affected by XSS worms. [Orkut](#) , [MySpace](#) (as well as a second possibility for a [QuickTime XSS flaw](#)), [GaiaOnline](#) , [Hi5](#) are just the tip of the iceberg, since a great deal of currently unfixed vulnerabilities can easily become XSS worms if that's what someone wants to achieve.

Adding a second layer of protecting for the end users, with the first one being the site's own responsibility for self-auditing themselves, widely used Internet browsers are finally contributing to the second layer of protection, with [Mozilla's Site Security Policy](#) and [IE8's Cross Site Scripting Filter](#) , aiming to protect the user [even if the site itself remains vulnerable](#) . Let's see how long before malicious parties start bypassing the built-in protection mechanisms, and publicly demonstrate this on a large scale.

XSS Flaw discovered in Skype's Shop, user accounts targeted | ZDNet

The independent security researcher [Ucha Gobejishvili](#) has [detected a cross site scripting \(XSS\) vulnerabilities](#) affecting **shop.skype.com** and **api.skype.com** .

Upon successful exploitation the vulnerability allows an attacker to hijack cookies via required user interaction, leading to complete session hijacking and stealing of the account.

Skype has been informed of the vulnerabilities and is currently investigating.

XSS bug in Skype for iPhone, iPad allows address book theft | ZDNet

A security researcher have [created a proof of concept code](#) that shows that a users AddressBook can be stolen from an iPhone or iPad.

The XSS bug is affecting the latest version of Skype for iOS, and works like that:

A Cross-Site Scripting vulnerability exists in the "Chat Message" window in Skype 3.0.1 and earlier versions for iPhone and iPod Touch devices. Skype uses a locally stored HTML file to display chat messages from other Skype users, but it fails to properly encode the incoming users "Full Name", allowing an attacker to craft malicious JavaScript code that runs when the victim views the message.

The researcher informed Skype of the issue on [24 August](#), and was told that an update to fix it would be released early in September.

[Watch a video demonstration of the XSS bug in action.](#)

WordPress releases version 3.5.1, fixes 3 security issues | ZDNet

Yesterday's release of [WordPress v3.5.1](#) , fixes 37 bugs, including three security issues.

The following security issues were addressed:

A server-side request forgery vulnerability and remote port scanning using pings. This vulnerability, which could potentially be used to expose information and compromise a site, affects all previous WordPress versions.

Two instances of cross-site scripting via shortcodes and post content.

A cross-site scripting vulnerability in the external library Plupload.

[Vulnerable WordPress installations](#) are a common target for cybercriminals, who regularly use them as a [foundation for launching malicious attacks](#) .

WordPress users are advised to upgrade to [the latest version](#) immediately, as well as to go through this [very informative article](#) , discussing the most common malware infections that could possibly affect them.

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

With or without McColo, spam volume increasing again | ZDNet

It was only a matter of time for spam volume to sky rocket again, despite [McColo's shutdown in November](#) . Two weeks after the cybercrime-friendly ISP got disconnected from the Internet, [spam volumes are increasing once again](#) with the main botnets using it as a command and control location regaining their strength by migrating to new hosting locations. Attempting to capitalize on the upcoming holidays, it took spammers two weeks to restore operations of the botnets responsible for a huge percentage of the spam messages globally. The attached graph courtesy of [SpamCop.net's Statistics](#) perfectly illustrates their motivation, with week 45 and week 46 indicating McColo's demise, and week 47 and 48 demonstrating continuity planning in action.

Let's take a brief retrospective at the two major cybercrime-friendly ISP clean up operations in 2008, and discuss the continuity planning strategies that they took advantage of.

Following the persistent reports issues by the security community for months, at the end of September, California based ISP Atrivo/Interpace was disconnected from the Internet by its upstream provider [causing only a brief disruption of spam levels](#) . The clean up operation continued, and in the middle of November the infamous [cybercrime friendly ISP McColo](#) that's been operating for years, was also disconnected from the Internet resulting in the first major spam decline for years.

With the botnet masters now unable to issue commands to the infected hosts, [hundreds of thousands of bots were unsuccessfully attempting to receive malicious instructions](#) from a location that was no longer online. At first, it would seem tha the security community got them off guard, but at a later stage it became evident the very same marginal thinking applied by Atrivo/Interpace who's been switching from upstream provider to upstream provide during the entire 2008, proved itself once again. [During the several hours](#) in

which they [managed to get McColo back online](#) , the botnet masters issued new commands making McColo's existence irrelevant to the overall continuity of the botnets operations. The owners of some of the botnets using McColo as a main command and control server then briefly started regaining control of them, with [Srizbi attempting to migrate to an Estonian ISP](#) , and [Rustock to LayeredTech](#) .

According to [Marshal's TRACE team's most recent stats](#) , of all the botnets that used to operate at McColo, Mega-D so far has been the only one to not only resume its operations, but to engage in more aggressive spamming than ever, currently representing 44.9% of spam activity from a single bot. As long as [the spammers and their customer base](#) aren't facing the music, it would simply be a game of cat and mouse.

With 256-bit encryption, Acrobat 9 passwords still easy to crack | ZDNet

Following ElcomSoft's claim that despite the 256-bit encryption [Acrobat 9 passwords are susceptible to more efficient brute forcing](#) than Acrobat 8 passwords -- a claim that Adobe [confirmed citing usability trade-offs](#) and urged users to take advantage of its improved passphrase mechanisms -- ElcomSoft's **Dmitry Sklyarov** and **Vladimir Katalov** provide more insights on the implications of their discovery, Adobe's reaction, and what should end users and companies do in order to balance security with usability.

Go through the Q&A.

Q: Could you please elaborate a bit more on what exactly does the vulnerability allows you, or a potential malicious attacker to do?

A: Passwords for PDF documents encrypted with AES-256 could be tested much faster than earlier. So, password that considered to be secure enough (difficult to find) in Acrobat 8 could become insecure (easy to find) in Acrobat 9.

Q: Have you contacted Adobe in regard to the vulnerability you've discovered, and did they confirm it?

A: Actually vice versa: Adobe representatives contacted us right after the press release with a question on vulnerability we discovered and we provided our technical clarifications. Yesterday there appeared an article on [Adobe corporate website](#) , which actually doesn't explain anything.

Q: Compared to Adobe Reader 8.0, how has your brute force rate improved by taking advantage of the flaw in numbers?

A : In Acrobat versions from 5 to 8, it was needed to make 51 MD5 calls and 20 RC4 calls, making password verification relatively slow, and so brute-force attacks were not effective -- only about 50,000 passwords per second on modern Intel processor, so even 6-character password was strong enough.

In Acrobat version 9, password checking routine consist of just one call to SHA256 hash function. That function can be implemented really effectively on all modern CPUs with SSE2 instruction set, with linear scalability on multi-core and multi-CPU systems, allowing to reach the speed from 5 to 10 million passwords per second. Moreover, SHA256 algorithm fits really good to stream processors such as ones used in NVIDIA video cards, reaching the speed of up to 100 million passwords per second on a single GPU, again with a linear scalability to multi-GPU systems and Tesla. That makes even 8-character password (mixed uppercase and lowercase letters) not secure.

To be more precise, Q6600 - iCore 4 cores on 2.4GHz :

Acrobat 8 ~ 56 700 p/s for user password Acrobat 9 ~ 5 100 000 p/s for user password on one core Acrobat 9 ~ 20 350 000 p/s on Q6600 (4 cores)

GPU GTX260 has 192 stream processors: Acrobat 9 ~ 74 500 000 p/s

You can see the difference.

Q: What should end user and companies do to ensure that their encrypted and password protected remain private, whereas they're still using the latest version of Adobe's product, potentially mitigating several known vulnerabilities found in the previous one?

A: AES-256 encryption introduced in Acrobat 9 does not significantly change level of document security. 256-bit encryption is stronger than 128-bit encryption used in previous versions of Acrobat. But it seems to be impossible to test all possible 128-bit keys in nearest future (several million years). So, Adobe just makes unbreakable thing stronger in Acrobat 9.

But actually security level is determined by the weakest link. In case if strong cryptography is used, the weakest link is a password - it could be guessed much easily than encryption key. Computers become faster every year. And common practice is to increase complexity of password testing process in new versions of software. But Adobe decided to make password testing faster. To preserve level of security provided by Acrobat 8 user just needs to use 128-bit

security (which still available in Acrobat 9). Or make new passwords several characters longer than earlier.

Windows 7's default UAC bypassed by 8 out of 10 malware samples | ZDNet

A recently conducted test by malware researchers reveals that [eight out of ten malware samples used in the test, successfully bypassed Windows 7's default UAC](#) (user access control) settings. The findings were also confirmed by a separate test done by another company, with an emphasis on how one of the most [popular scareware variants bypassed Windows 7's default UAC's settings](#) as well.

More info:

On October 22nd, we settled in at SophosLabs and loaded a full release copy of Windows 7 on a clean machine. We configured it to follow the system defaults for User Account Control (UAC) and did not load any anti-virus software.

We grabbed the next 10 unique samples that arrived in the SophosLabs feed to see how well the newer, more secure version of Windows and UAC held up. Unfortunately, despite Microsoft's claims, Windows 7 disappointed just like earlier versions of Windows. The good news is that, of the freshest 10 samples that arrived, 2 would not operate correctly under Windows 7.

The findings are in fact not surprising, since the main problem with Windows 7's UAC lies in the over-expectation of the average end user. Just like [free antivirus software](#) relying entirely on [signatures based scanning only](#), the over-expectation of Windows 7's UAC may in fact fool a large number of users that third-party security software is not a necessity.

Just like end users, enterprises already migrating to Windows 7 face the same security issues. Eric Voskuil, CTO, BeyondTrust -- the company that issued a report earlier this year, claiming that [92% of critical Microsoft vulnerabilities are mitigated by Least Privilege accounts](#) -- believes that the required administrator privileges for using the feature [may in fact pose new security challenges](#) :

In response to feedback that users were forced to respond to too many prompts in Windows Vista, the new operating system introduces a new approach to User Account Control (UAC), providing a four-position “slider” feature to control how often UAC pop-ups occur. While these changes to Windows 7’s UAC benefit the home user market, enterprises must recognize that the new slider feature can only be applied to users logged in as administrators and may increase security risks.

Further, Windows 7 introduces no new features to solve the application compatibility issues experienced by standard users in previous versions of the operating system. “The most secure configuration option for enterprises that deploy Windows 7 remains running end-users as standard users, with administrator rights removed,” said Eric Voskuil, CTO, BeyondTrust.

What do you think about Windows 7's user access control slider? Is it a step in the right direction, or does it have the potential to provide a lot of users with a false feeling of security, making them believe that a stand-alone HIPS (host based intrusion prevention/behavior blocking) solution isn't necessary?

TalkBack.

Winamp 5.63 fixes four critical security vulnerabilities | ZDNet

[Winamp](#) users, it's time to upgrade to the latest version of the popular audio and video player.

As originally reported in [Winamp's release announcement](#), version 5.63 fixes four critical security vulnerabilities. Successful exploitation of the vulnerabilities allows execution of arbitrary code. For the exploitation to take place, a user running an outdated version of Winamp, would have to open a specially crafted . AVI video file.

More details about the vulnerability can be found in this [Secunia advisory](#).

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Who's behind the GPcode ransomware? | ZDNet

In one of these moments when those who are supposed to know, don't know, and those who don't realize what they know

aren't reaching the appropriate parties, it's time we get back to the basics - finding out who's behind GPcode, and trying to tip them on the consequences of their blackmailing actions in between collecting as much actionable intelligence as possible using [OSINT](#) (open source intelligence) and [CYBERINT](#) (cyber intelligence practices).

[Great situational awareness](#) on behalf of Kaspersky Labs who were the first to report that a new version of GPcode (also known as PGPCoder) is in the wild, this time with a successful implementation of RSA 1024-bit encryption. However, aiming to crack the encryption could set an important precedent, namely using distributed computing to fight the effect of cyber criminal's actions. Theoretically, the next time they'll introduce even stronger encryption, which would be [impossible to crack](#) unless we want to end up running a dedicated [BOINC project cracking ransomware](#) in the future. Are there any other more pragmatic solutions to dealing with cryptoviral extortion? It's all a matter of perspective. More info on the [Stop GPcode initiative](#) , seeking and receiving the collective intelligence of independent researchers in this blog post :

"Along with antivirus companies around the world, we're faced with the task of cracking the RSA 1024-bit key. This is a huge cryptographic challenge. We estimate it would take around 15 million modern computers, running for about a year, to crack such a key. Of course, we don't have that type of computing power at our disposal. This is a case where we need to work together and apply all our collective knowledge and resources to the problem. So we're calling on you: cryptographers, governmental and scientific institutions, antivirus companies, independent researchers...join with us to stop Gpcode. This is a unique project – uniting brain-power and resources out of ethical, rather than theoretical or malicious

considerations. Here are the public keys used by the authors of Gpcode."

Despite that GPcode indeed got the encryption implementation right this time, it's only weakness remains the way it simply deletes the files it has just encrypted, next to securely wiping them out - at least according to a single sample obtained. Consequently, just like a situation where your files are encrypted with strong encryption and virtually impossible to crack, but the original files. Moreover, instead of trying to crack an algorithm that's created not to be cracked at least efficiently enough to produce valuable results by have the encrypted data decrypted, why not buy a single copy of the decryptor and start analyzing it? It also appears that the decryptor isn't universal, namely they seem to be building custom decryptors once the public key used to encrypt the data has been provided to them.

So, the ultimate question - who's behind the GPcode ransomware? It's Russian teens with pimples, using E-gold and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either \$100 or \$200 for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the email responses they sent back, the currency accounts, as well their most recent IPs used in the communication :

Emails used by the GPcode authors where the infected victims are supposed to contact them : content715@yahoo .com
saveinfo89@yahoo .com cipher4000@yahoo .com
decrypt482@yahoo .com

Virtual currency accounts used by the malware authors :
Liberty Reserve - account U6890784 E-Gold - account - 5431725 E-Gold - account - 5437838

Sample response email : *"Next, you should send \$100 to Liberty Reserve account U6890784 or E-Gold account 5431725 (www.e-gold.com) To buy E-currency you may use exchange service, see or any other. In the transfer description specify your e-mail. After receive your payment, we send decryptor to your e-mail. For check our guarantee you may send us one any encrypted file (with cipher key, specified in any !_READ_ME_!.txt file, being in the directorys*

with the encrypted files). We decrypt it and send to you originally decrypted file. Best Regards, Daniel Robertson "

Second sample response email this time requesting \$200 :

"The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com). 3. If you do not make one of this variants, contact us for decision it. For check our guarantee you may send us ONE any encrypted file. We decrypt it and send to you originally decrypted file. For any questions contact us via e-mail. Best regards. Paul Dyke "

So, you've got two people responding back with copy and paste emails, each of them seeking a different amount of money? Weird. The John Dow-ish Daniel Robertson is emailing from **58.38.8.211** (Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), and Paul Dyke from **221.201.2.227** (Liaoning Province Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), both Chinese IPs, despite that these campaigners are Russians.

This incident is a great example of targeted cryptoviral extortion attacks, namely, it's not efficiency centered and the core distribution method remains unknown for the time being. Analysis and investigation is continuing. If you're affected, look for backups of your data, or try restoring the deleted files, don't stimulate blackmailing practices by paying them.

Who keeps failing their FISMA compliance? | ZDNet

The recently released [U.S Federal Computer Security Report Card for 2008](#) , indicates that several critical to national security departments continue failing to implement the [Federal Information Security Management Act \(FISMA\)](#) .

From a cyber espionage perspective, the lack of prioritization of departments that must be audited first, often results in anecdotal cases.

Case in point, who cares if the Environmental Protection Agency scored A+ when the Nuclear Regulatory Commission and the Department of the Interior have been failing for 2006 and 2007 altogether? And isn't it disturbing to know that Housing and Urban Development scores higher than the Department of Defense? Secured by default through the use of (outdated) information security acts isn't perfect, and the results of such assessments shouldn't be taken for granted. That's mostly because the threatscape and the dynamic development of a department's infrastructure is prone to grow faster than a standard can keep up with the threats and insecurities posed by the new technologies. Here are some more opinions about FISMA's applicability in real-life threatscape situations :

“Some argue that FISMA does not adequately measure information security,” said Tim Bennett, president at the Cyber Security Industry Alliance. “A high FISMA grade doesn’t mean the agency is secure and vice versa. That is because FISMA grades reflect compliance with mandated processes: they do not, in my view, measure how much these process have actually increased security.” Despite an obvious need to improve security, no one suggested scrapping FISMA.

“The bill itself is fine with the way the framework is set up,” said Karen Evans, OMB’s administrator for electronic government and IT. FISMA is a tool that provides metrics for reporting efforts, and with

independent IG evaluations it does not rely on self-reporting. Whether or not it is a paperwork drill or a genuine enhancement to security “depends on how the agency goes about doing the work.”

[FISMA is currently revisited](#) , and therefore [an updated framework](#) is definitely in the works.

Which is the most popular malware propagation tactic? | ZDNet

According to [Microsoft's recently released Security Intelligence Report](#), that's socially engineered malware ([scareware pop ups](#); blackhat search engine optimization attacks), or malware requiring user interaction such as campaigns enticing users into [downloading and executing a malicious file](#).

More propagation tactics:

- User Interaction required - 44.8%
- AutoRun USB - 26%
- AutoRun: Network - 17.2%
- File Infector - 4.4%
- Exploit: Update Long Available - 3.2%
- Exploit: Update Available - 2.4%
- Password Brute Force - 1.4%
- Office Macros - 0.3%
- Exploit: Zero Day - 0%

Based on a sample of 600 million systems worldwide, the research further positions AutoRun USB infection as the second most popular malware propagation tactic, based on the data provided by the software giant. [Microsoft disabled AutoRun by default on Windows XP/Vista in February](#) in order to prevent malware infections. The results, at least according to Microsoft, have indicated [a significant decline in malware](#) using AutoRun as a spreading mechanism.

The report also points out that zero day flaws do not necessarily represent a driving force in the growth of malicious attacks or cybercrime in general. A point -- including several other -- which I already discussed in my article "[Seven myths about zero day vulnerabilities debunked](#)".

How well is Microsoft positioned to take advantage of the points presented in the study? For starters, for a second year in a row, [Microsoft's Internet Explorer outperforms competing browsing](#)

[in protecting against socially engineered malware](#), at least according to studies conducted by NSS Labs. Studies whose methodology I debunked in related posts - "[IE8 outperforms competing browsers in malware protection -- again](#)" ; "[Study: IE8's SmartScreen leads in malware protection](#)".

Now that socially engineered malware is supposedly taken care of, what else is Microsoft missing? It's malware that spreads without user interaction, namely through the [exploitation of client-side vulnerabilities](#) in [third-party software](#) and [browser plugins](#). That's precisely what the studies from NSS Labs have omitted from their research, especially in times when web malware exploitation kits dominate the threatscape.

What are some of the most common client-side exploits that malicious attackers attempt to exploit through these kits? According to Microsoft:

The most commonly observed type of exploits in 1H11 were those targeting vulnerabilities in the Oracle (formerly Sun) Java Runtime Environment (JRE), Java Virtual Machine (JVM), and Java SE in the Java Development Kit (JDK). Java exploits were responsible for between one-third and one-half of all exploits observed in each of the four most recent quarters.

Consider going through the report [here](#).

Which is the most popular antivirus software? | ZDNet

In an over-crowded antivirus software market, end and corporate users are often finding it difficult to differentiate between a value-added market proposition, next to the "me too" vendors of solutions. As in every other market segment, any scientific insight into the market share of various vendors offers an invaluable perspective into the market dynamics, what are customers purchasing, and most importantly, are they living in a world of 'false feeling of security'.

Using a data set consisting of 120,000 data points, [researchers from OPSWAT recently released an informative overview of the antivirus market](#), answering an important question - which is the most popular antivirus vendor?

According to their findings, that's avast! Free Antivirus, followed by Microsoft Security Essentials and ESET NOD32 Antivirus.

Detailed market share statistics:

- Avast - 17.4% worldwide market share
- Microsoft - 13.2% worldwide market share
- ESET - 11.1% worldwide market share
- Symantec - 10.3% worldwide market share
- AVG - 10.1% worldwide market share
- Avira - 9.6% worldwide market share
- Kaspersky - 6.7% worldwide market share
- McAfee - 4.9% worldwide market share
- Panda - 2.9% worldwide market share
- Trend Micro - 2.8% worldwide market share
- Other - 11.1% worldwide market share

Microsoft is the market leader in North America, followed by Symantec and AVG. Not surprisingly, the market leading avast! Free Antivirus is relying on the so called "freemium" business model, where the company grows and gains market share by offering a free alternative of their software, and earns revenue thanks to the successful conversion of free users to paid ones. Earlier this year,

the company announced that it has [150 million active users worldwide](#), a clear indication of a working "freemium" business model.

Go through related Image Galleries:

[Image Gallery: Avast! Antivirus office in Prague, Czech Republic](#)
[Image Gallery: The \(European\) Antivirus market - current trends](#)

Just how relevant is antivirus nowadays? In a recently released study entitled "[Measuring the Cost of Cybercrime](#)", researchers argue that less money should be spent on purchasing antivirus software, and more money in tracking down and prosecuting cybercriminals. Next to these conclusions, [F-Secure's Mikko Hypponen](#) recently admitted that [antivirus software failed in Stuxnet and Flame's cases](#), provoking more discussion on the actual applicability of antivirus software in today's mature cybercrime ecosystem.

What do you think? Is antivirus software still relevant in the age of Stuxnet, Duqu and Flame, the so called poster kids of the DIY targeted attack toolkits and weaponized malware releases? Do think free antivirus is offering a 'false feeling of security' compared to subscription based license models?

TalkBack!

Find out more about Dancho Danchev at his [LinkedIn profile](#), or [follow him on Twitter](#).

Which are the most commonly observed Web exploits in the wild? | ZDNet

M86Security's newly released report "[Security Labs Report - July - December 2011 Recap](#)", details some of the most commonly observed Web exploits currently in the wild, as well as offers a detailed overview of the most popular web malware exploitation kits.

Some of the most commonly observed exploits are:

- Microsoft Internet ExplorerRDS ActiveX - 17.7%
- Java WebStart Arbitrary Command Line Injection - 6.3%
- Microsoft Internet Explorer user Data Behavior - 4.7%
- Cloned DOM Object Malformed Reference - 4.2%
- Office Web Components Active Script Execution - 3.9%
- Microsoft Internet Explorer Self-Executing HTML Arbitrary Code Execution - 3.4%
- Adobe Acrobat and AdobeReader CollectEmailInfo JavaScript method buffer overflow - 2.2%
- Adobe Reader util.printf()JavaScript Function StackOverflow - 1.3%
- Adobe Reader media.newPlayer - 1.3%
- Microsoft Internet ExplorerTable Style Invalid Attributes - 1.1%
- Adobe Reader GetIconJavaScript method buffer overflow - 1.1%
- Java Plugin Web Start Parameter - 1.0%
- Windows Help and SupportCenter Protocol Handler - 0.9%
- Microsoft Internet ExplorerDeleted Object EventHandling - 0.8%
- IE STYLE Object InvalidPointer ReferenceVulnerability - 0.6%

More from M86Security's report:

Exploits in the second half of 2011 targeted a variety of products, including Microsoft Internet Explorer, Oracle Java, Microsoft Office productsand quite commonly, Adobe Reader and Adobe Flash. Security fixes for some of these vulnerabilities have been available for years, whichpoints out a continuous problem: Many users and organizations do not patch all their installed software in a timely manner, and attackersleverage this weakness to their advantage.As

the table shows, more than half of the most exploited vulnerabilities are used by the prevalent Blackhole exploit kit.

Based on the report, the BlackHole web malware exploitation kit remains the most popular client-side exploits serving kit, representing 95.1% of observed malicious URLs. M86Security contributes the growth of the BlackHole web malware exploitation kit due to the frequent updated issues by the coders of the kit, including the very latest remotely exploitable vulnerabilities.

The report's findings [confirm the findings from previously released reports](#) indicating that [outdated and already patched vulnerabilities remain among the key driving forces](#) for the success of cybercrime.

End users are advised to ensure that they're running [the latest versions of popular software](#), as well as [browser plugins](#), to avoid exploitation through client-side exploits.

Which antivirus is best at removing malware? | ZDNet

Detecting the presence of malicious code is one thing, successfully eradicating it is entirely another.

According to AV-Comparatives.org/s recently released malware removal test evaluating [the effectiveness of sixteen antivirus solutions](#) , only a few were able to meet their criteria of not only removing the FakeAV, Vundo, Rustock and ZBot(Zeus) samples they were tested against, but also getting rid of the potentially dangerous "leftovers" from the infection.

More info on the tested antivirus solutions , and how they scored:

The test, including the following antivirus solutions - *Avast Professional Edition 4.8 ; AVG Anti-Virus 8.5 ; AVIRA AntiVir Premium 9.0 ; BitDefender Anti-Virus 2010 ; eScan Anti-Virus 10.0 ; ESET NOD32 Antivirus 4.0 ; F-Secure AntiVirus 2010 ; G DATA AntiVirus 2010 ; Kaspersky Anti-Virus 2010 ; Kingsoft AntiVirus 9 ; McAfee VirusScan Plus 2009 ; Microsoft Security Essentials 1.0 ; Norman Antivirus & Anti-Spyware 7.10 ; Sophos Anti-Virus 7.6 ; Symantec Norton Anti-Virus 2010 ; Trustport Antivirus 2009* , relied on a modest malware sample, whose prevalence is however easily seen in the wild these days.

Their conclusion:

"None of the products performed "very good" in malware removal or removal of leftovers, based on those 10 samples. **eScan, Symantec and Microsoft (MSE) were the only products to be good in removal of malware AND removal of leftovers.** Due to the sample size, the final ratings may be generous, but we applied the scoring tables strictly. We tried to give different values for different types of leftovers, although this was very difficult in some gray area cases.

This was the first public malware removal test of AV-Comparatives and due the lack of generally accepted ways to rate malware removal abilities, we did out best to give a fair rating based on the

observed overall malware removal results and to do not look / base out ratings on e.g. the deletion of the binary malware only."

It's worth keeping in mind that [the timeliness of these comparative reviews](#) in an ever-changing threat-scape should be consider before jumping to any conclusions. For instance, [quality assurance aware cybercriminals](#) rely on [underground alternatives](#) of the popular [VirusTotal](#) service, allowing them to [pre-scan their malware releases](#) before including them in a campaign.

Go through related posts: [MS Security Essentials test shows 98% detection rate for 545k malware samples](#) ; [Does free antivirus offer a false feeling of security?](#) ; [Does software piracy lead to higher malware infection rates?](#) ; [Modern banker malware undermines two-factor authentication](#) ; [Commonwealth fined \\$100k for not mandating antivirus software](#)

The bottom line - [prevention is always better than the cure](#) , which in terms of malware means operating on an up-to-date operating system, that's also [free of third-party application](#) and browser [plug-in vulnerabilities](#) , followed by a decent [situational awareness](#) on [their current tactics](#) , and basic understanding that the antivirus software is only a part of [the defense in-depth solution](#) .

Web malware exploitation kits updated with new Java exploit | ZDNet

Cybercriminals are quick to capitalize on the announcement of a newly discovered vulnerability -- [CVE-2011-3544](#) -- in Java.

[According to researchers from M86Security](#), popular web malware exploitation kits such as Phoenix exploit kit 3.0 and the Blackhole Exploit Kit version 1.2.1 were updated with a new recent exploit before a patch had been released.

Does this mean that cybercriminals are actively relying on zero day flaws as a success factor for their malicious campaigns? Not at all, as [zero day flaws are not the primary growth factor of the cybercrime ecosystem](#). Instead, the cybercriminals rely on already patched vulnerabilities, whose active exploitation is the primary objective of web malware exploitation kits.

Based on [third-party research](#) from [multiple sources](#), we can clearly conclude that end users aren't patching their third-party applications and browser plugins, making it fairly easy for cybercriminals to actively exploit this trend.

Related posts:

[37 percent of users browsing the Web with insecure Java versions](#)
[56 percent of enterprise users using vulnerable Adobe Reader plugins](#)
[Kaspersky: 12 different vulnerabilities detected on every PC](#)
[Report: malicious PDF files becoming the attack vector of choice](#)
[Report: Patched vulnerabilities remain prime exploitation vector](#)

Weak passwords dominate statistics for Hotmail's phishing scheme leak | ZDNet

The [recently leaked](#) accounting [data of thousands](#) of Hotmail users -- Gmail has [also been affected](#) -- obtained through what appears to be a badly executed phishing campaign, once again puts the spotlight on the how [bad password management practices](#) remain an inseparable part of the [user-friendly ecosystem](#) .

According to a [statistical analysis of the 10,000 passwords](#) published by Bogdan Calin at Acunetix, 42% of the phished users use lower alpha passwords only (a to z), 19% rely on numbers only, with 22% of the total sampled population using a 6 character password (Live.com's minimum), followed by 21% of users using 8 character passwords.

Here are the top 10 most commonly used passwords:

- 123456 - 64 - 123456789 - 18 - alejandra - 11 - 111111 - 10 - alberto - 9 - tequiero - 9 - alejandro - 9 - 12345678 - 9 - 1234567 - 8 - estrella - 7

And whereas brute-forcing email accounts on a mass scale has been replaced by the much more efficient and [automated approach of registering new accounts](#) , the weak password management practices used by the affected users combined with the fact that users continue [using the same password](#) across [different services](#) , can create a favorable chain reaction for a cybercriminal knowing this simple fact.

Go through related posts: [Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers](#) ; [Spammers attacking Microsoft's CAPTCHA -- again](#) ; [Microsoft's CAPTCHA successfully broken](#) ; [Lack of phishing attacks data sharing puts \\$300M at stake annually](#) ; [Online broker CommSec criticised for weak passwords, lack of SSL](#) ; [Study: password resetting 'security questions' easily guessed](#) ; [Comcast responds to passwords leak on Scribd](#)

Does the size and complexity of a password matter in the case of online brute-forcing? It depends, in the sense that if the end user

believes he's visiting the legitimate site, not even a 15 character password will prevent a phisher from obtaining it, even worse if the end user is malware-infected, the cybercriminal wouldn't even bother launching a phishing campaign at the first place. What he shouldn't be able to do that easily through phishing, is obtain access to all the services in use by the phished user relying on a single password.

Despite the fact that Hotmail allows users the option to [set a password to expire every 72 days](#) , isn't it time that Microsoft empowers its users with a Gmail-like "[recent account activity](#)." feature?

What do you think? Talkback.

Wardriving police: password protect your wireless, or face a fine | ZDNet

Internet users in Germany, whose wireless networks are left password unprotected, can be fined up to [100 euros](#), according to [a recent ruling by Germany's top criminal court](#).

The ruling is in response to a musician's lawsuit against a user whose [unprotected wireless network was used for](#) downloading and sharing music over P2P.

Just how realistic is the ruling, from a security perspective? Is a weak password protected wireless network, any different than the one with no password security at all?

"Private users are obligated to check whether their wireless connection is adequately secured to the danger of unauthorized third parties abusing it to commit copyright violation," the court said. Internet users can be fined up to euro 100 (\$126) if a third party takes advantage of their unprotected WLAN connection."

The ruling is not just missing the emphasis on the importance of strong passwords, but it also *"doesn't expect users to constantly update the security of their wireless networks"*. Moreover, it's not even building awareness on the fact how [the choice of the encryption protocol](#), can greatly slow down a potential attacker, in a combination with strong password.

With [GPU-accelerated WiFi password recovery speeds](#) prone to increase over time, as well as the [increasing availability](#) of [DIY cracking kits](#), emphasizing on [the use of strong passwords](#) in a combination with with right encryption protocol, next to [basic MAC address filtering](#), is the right security awareness building approach.

The main problem with insecure wireless networks, is the fact that malicious [wardrivers](#) can easily forward the responsibility for their activities to the owner of the unsecured wireless network.

[For instance, in 2008](#) :

It became evident that a group of Indian militants [took unethical hacking courses](#) , and once learning the basics of wardriving, used the [insecure wireless network of a U.S expatriate](#) to send [emails claiming responsibility](#) for serial bombings that took place in July and September -

“Roaming around Mumbai with Wi-Fi detectors, the suspects looked for open Wi-Fi signals and programmed the e-mail messages to be sent from hacked wireless networks prior to the blasts, the Indian police said. The technique used by the militants is similar to “wardriving,” where hackers roam around to detect and access Wi-Fi networks with security weaknesses.”

The "wardriving police unit" is not a new concept. The first time I heard about it, was in 2006, when the [Douglas County Sheriff's Department was considering to scan for insecure wireless networks](#) , and drop off brochures with instructions on how to properly secure them.

Three years later, [Mumbai's police started implementing the practice](#) , in response to the abuse of insecure wireless networks by Indian militants:

Additional Commissioner of Mumbai Police K Venktesan told Business Standard: “If the Wi-Fi connection in a particular place is not password protected or secured then the policemen accompanying the squad will have the authority to issue a notice to the owner of the connection directing him to secure it.”The police could issue a notice under section 149 of the Criminal Procedure Code (CrPC) to anyone found not securing their Wi-Fi connection and user may face criminal investigations.

Again in 2009, the [Australian police also planned similar wardriving sessions](#) :

The Queensland Police plans to conduct a 'wardriving' mission around select Queensland towns in an effort to educate its citizens to secure their wireless networks. When unsecured networks are found, the Queensland Police will pay a friendly visit to the household or small business, informing them of the risks they are exposing themselves to.

Although the problem with insecure wireless networks is often greatly underestimated, the big picture has to do with the fact that, when there are hundreds of thousands of password-unprotected wireless networks, this well known fact allows malicious attackers to efficiently propagate wireless malware. Related [studies done on the subject](#), prove just how easy it is to [execute such a malware campaign](#).

What do you think?

Does the "Wardriving police" concept have any future? Is your neighbor's insecure wireless network setting up the foundations for a cybercrime-friendly infrastructure, or are there much more important issues to take care of first, before starting to drop off "*Insecure Wireless Network Detected!*" brochures?

UPDATED: Several German readers have contacted me, since they believe the story was misinterpreted in a way that it makes it sounds as if the German police is wardriving around, looking for insecure wireless networks, and fining their owners:

"The music company and a troll demanded \$250k compensation and damages. The owner appealed, and eventually reached the highest German court. This rejected the music company's claim, but ruled that the owner of a WLAN had a duty to secure the WLAN with the usual techniques at the installation time. The second ruling limited the liability of the WLAN owner for misuse by war drivers to 100 Euro, about \$120. This is NOT a fine, and it doesn't mean that the police will look for unsecured WLANs and fine the owner."

The angle of this article was to emphasize on the increasing policing of insecure wireless networks across the globe with India and Australia cited as examples, the potential for forwarding the responsibility for malicious actions that took place over the insecure network to its owner in the context of the ruling, the futility of offering password protection advice without emphasizing on strong passwords in terms of the ever-improving brute forcing speeds, and to facilitate a conversation on the pros and cons of the "wardriving police unit" trend, clearly seen across the globe.

Talkback, and share you opinion.

Image courtesy of [ElcomSoft's GPU-accelerated wireless security auditor](#) .

Waledac botnet spamming fake SMS spying tool | ZDNet

Waledac is once [again using](#) its [well](#) proven [social engineering tactics](#) by introducing a "[fake SMS spying tool](#) " ([free.exe](#) ; [smstrap.exe](#) ; [install.exe](#) ; [setup.exe](#) etc.) and [Online Casinos theme](#) , in an attempt to further [expand the botnet](#) .

No client-side vulnerabilities are used for the time being, instead the cybercriminals are relying on their persistent rotation of the themes, and the end user's lack of awareness.

Here are more details on the subjects/message used:

Typical spam subjects used:

Can your love life be re-ignited? Are you sure in your partner's faithfulness? Now, It's possible to read other people's SMS We will tech you to be the master of making love art Just type the phone number and read SMS Do you want to test your partner? Have more fun and pleasure in your intimate life Now, you can read any SMS messages from any mobile phones Keep a spy eye on your Girlfriend's mobile What's Your Hall of Shame Are you redy to know the truth?

The message itself:

"Get Your Free 30-Day Trial! Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner. Just download the program and you will able to read all SMS when you are online. Be aware of everything! This is an extremely new service!"

Having migrated from a P2P communications model to a web based communications model (see live sample of Waledac attempting to connect to infected hosts), taking into consideration the similarities in the spam templates used, as well as network level connections, [Waledac may not just be a successor to the Storm Worm](#) , but may in fact be a reincarnated version of Storm.

Go through related Storm Worm posts: [Legal concerns stop researchers from disrupting the Storm Worm botnet](#) ; [The Storm Worm would love to infect you](#) ; [Tracking down the Storm Worm malware](#) ; [Storm Worm's Independence Day campaign](#) ; [Storm Worm says the U.S have invaded Iran](#)

Interestingly, Waledac is an example of a botnet that's propagating by rubbing shoulders with some of the most prolific botnets currently in circulation, including the Conficker, with the most [recent variant pushing a Waledac sample](#) , presumably under a business agreement with Conficker's authors looking for more ways to monetize the botnet. Moreover, according to [Microsoft's MMPC](#) , in the past they "*observed malware such as [Win32/Bredolab](#) download and install Waledac. Bredolab is notorious for installing prevalent spam bots such as Rustock, Cutwail, Srizbi, Tedroo and Rlsloup.*"

This ongoing cooperation proves that while certain cybercriminals are still living in the "no honor among cybercriminals" world by attempting to scam one another ([Phishers increasingly scamming other phishers](#)) and [hijack each other's botnets](#) , the rest are clearly working together.

Vodafone HTC Magic shipped with Conficker, Mariposa malware | ZDNet

Just when you thought you have taken care of all the possible malware infection vectors, flawed quality assurance procedures once again demonstrate the need for a transparent and systematic approach of ensuring that digital devices are shipped malware-free.

In a new blog post, researchers from PandaSecurity are reporting on [Conficker, Mariposa and Lineage password stealing malware](#) samples, shipped with a recently purchased Vodafone HTC Magic smartphone.

More details:

Today one of our colleagues received a brand new Vodafone HTC Magic with Google's Android OS. The interesting thing is that when she plugged the phone to her PC via USB her Panda Cloud Antivirus went off, detecting both an autorun.inf and autorun.exe as malicious. A quick look into the phone quickly revealed it was infected and spreading the infection to any and all PCs that the phone would be plugged into. Interestingly enough, the Mariposa bot is not the only malware I found on the Vodafone HTC Magic phone. There's also a Conficker and a Lineage password stealing malware.

This is not an isolated incident, but an emerging trend. Over the past several years, a multitude of different devices have been shipped with malware that made its way through flawed quality assurance procedures.

Here's a brief retrospective of reported cases where digital devices were shipped with malicious software:

2006 - [Small Number of Video iPods Shipped With Windows Virus](#)
2006 - [McDonalds' free Trojan: "Would you like malware with that?"](#)
2007 - [TomTom ships malware on sat-nav](#) **2007** - [Seagate ships virus-infected hard drives](#) **2008** - [HP ships USB sticks with malware](#)
2008 - [Best Buy issues security warning on Insignia digital picture frames](#) **2008** - [Asus ships Eee Box PCs with malware](#) **2008** - [Samsung Digital Photo Frame shipped with malware](#) **2008** - [Malware](#)

[found in Lenovo software package 2008](#) - [Telstra distributes malware-infected USB drives at AusCERT 2009](#) - [Malware Found On Brand-New Windows Netbook \(M&A Companion Touch\)](#)

The Vodafone HTC Magic incident is the second for March, 2010, following the recently reported [malware infected Energizer DUO USB battery charger](#) .

Vishing attack on Skype pushing scareware | ZDNet

Multiple users are reporting on an ongoing [vishing attack](#) at Skype, attempting to [social engineer users into thinking they're infected with malware](#).

Here's how it works - victims typically receive a pre-recorded Skype call telling them they are infected with malware and need to visit a specific site:

Hey guys,I am working from home on my BlueCoat laptop. It has the cloud client on it. I have skype on this machine. I get a skype call from a place I didn't recognize. I answer the call and it is a recorded message. It says I have a fatal virus that needs to be fixed. That I am on Windows7. (I am not.) The recorded message tells me to go to www.helps.com. ... Can you find anything in our logs about what just happened? Thoughts?

The specific site in question is an online shop pushing rogue AV products and malware cleanup services.

The web sites - ***helps.com*** mentioned in the vishing attack is currently offline.

Have you been a victim of vishing attacks? How did you respond?

Talkback.

Vint Cerf's Twitter account hacked, suspended for spam | ZDNet

(UPDATE: [Cerf denies](#) that this was [his](#) Twitter [profile](#)) It appears that Vint Cerf, [the father of Internet](#) who needs no introduction, has had his [Twitter account compromised](#) , with a multitude of spam messages posted on his behalf during the last 24 hours, all of which are redirecting to auction search sites ([baysearch .net](#) and [soldly .com](#)). Cerf joined Twitter as of November this year [according to the Daily Follow](#) , with his account [currently suspended](#) due to the automated fashion in which the spam messages were posted. Shame on them.

The automated suspension appears to have been triggered because identical messages were posted within one minute interval for several hours such as :

"Have you heard about" "My friend mentioned" "Can't stop thinking about" "Have you seen"

This is not your typical high profile incident or yet another web malware exploitation kit released in the wild with Christmas promotion. This is pure irony, as the spammers that took control of the account and started spamming from it, wouldn't exist at the first place if it wasn't him who made it possible for them to blossom.

Verizon, Telecom Italia, and Brasil Telecom top the botnet charts in Q2 of 2008 | ZDNet

When was the last time you heard something in the lines of "*We do our best to protect our customers from the threats posed by...*" ? In reality though, the statement should end up like "*protect our customers from the threats posed by the rest of our customers*". [China may be hosting most of the web sites spreading malware](#) in one way or another, but if we're to consider the micro environment, the ISPs found to be hosting the most malware infected hosts on a per country basis during the last 30 days, are always worth pointing out.

CommTouch's recently released "[Second Quarter 2008 Email Threats Trend Report](#)" states that according to their sensors network :

"At the end of Q2, Turkey had moved into first place for the highest number of zombies (11% of all zombies worldwide), followed closely behind by Brazil and Russia with 8.4% and 7.4% respectively. Interestingly, the United States has fallen into ninth place, with only 4.3% of all zombies, compared to 5% in Q1 2008."

Wonder which ISPs were hosting the most malware infected hosts in Q2 of 2008?

"1 - ttnet.net.tr - 1,807,935 2 - telecomitalia.it - 1,219,940 3 - tpnet.pl - 1,162,406 4 - 163data.com.cn - 754,466 5 - telesp.net.br - 696,961 6 - asianet.co.th - 647,778 7 - brasiltelecom.net.br - 646,979 8 - verizon.net - 556,040 9 - speedy.net.pe - 564,599 10 - etb.net.co - 561,531"

This sample demonstrates the true international diversity of ISPs who manage botnet infrastructures for malware authors due to their inability to deal with already malware infected users, or the lack of incentives in the form of enforced legislation for them to do so. The numbers should be taken as very conservative mostly because of the fact that they are based on a single vendor's sensor network, and therefore, if more vendors exchange data and remove the

duplicates, the numbers are prone to increase. And with botnet masters continuing to abuse an Internet Service Provider's infrastructure in between degrading the quality of the service for all the customers, it's no surprise that [76.5% of email sent globally in June was spam](#) , with Switzerland as the most spammed country in the world. Theoretically, the spam and phishing emails a malware infected user receive, may in fact be coming straight from his own malware infected PC abused for the purpose of sending out scams, even locally hosting them.

The bottom line - should a country be blamed for neglecting its obligation to enforce local ISPs to "save their customers from themselves", or it's in fact the ISPs that should be named and shamed for maintaining botnet infrastructures on their networks as often as possible?

Vendor claims Acrobat 9 passwords easier to crack than ever | ZDNet

Password recovery software vendor [ElcomSoft](#) claims that the password verification mechanism in the new Adobe Acrobat 9 is weaker than the one used in the previous version of Adobe's product, thereby allowing them to improve the brute forcing speed a hundred times faster. The company's claim comes right after Adobe's implementation of 256-bit encryption in their Acrobat 9. A PR campaign promoting ElcomSoft's new product, or actual evidence of a flawed implementation on behalf of Adobe?

According to the company, [Adobe Acrobat 9 passwords are a hundred times easier to crack](#) than the ones in Acrobat 8 :

"ElcomSoft has discovered that the new PDF protection system implemented in Acrobat 9 is even faster to recover than in previous versions. In fact, a hundred times faster. "The new version of Adobe Acrobat is easier to break", claims ElcomSoft CEO Vladimir Katalov, quoting a speed increase of two orders of magnitude for the new format. "The new product has surprisingly weak protection", he adds. According to ElcomSoft's CEO, using 256-bit AES encryption per se is not enough to achieve ultimate security without employing complex approach and consideration of the entire security system. "

Yesterday, [Adobe issued a statement](#) commenting on their implementation of the 256-bit encryption, confirming the trade-off that they made so that 256-bit password protected documents could open faster in Acrobat 9, whereas password recovery tools could indeed achieve better brute forcing speed :

"The [current specification](#) for password-based 256-bit AES encryption in PDF provides greater performance than the previous 128-bit AES implementation. **While this allows for 256-bit AES password protected documents to open faster in [Acrobat 9](#) , it can also allow external brute-force cracking tools to attempt to guess document passwords more rapidly because fewer processor cycles are required to test each password guess.**

These tools operate independently of Acrobat and work directly on a password protected document by repeatedly guessing from lists of dictionary words like "turkey", "potato", and "pie" to see if the document will open."

In order for Adobe to balance usability with security, they improved the passphrase possibilities by introducing new characters and extending the previously limited length of the passphrase, potentially undermining brute forcing attempts in cases where quality passphrases are used. Sadly, that's not always the case. With a great number of people still (conveniently) choosing passwords over passphrases, their encrypted files still remain susceptible to successful brute forcing attempts. Why are passwords chosen over passphrases at the first place? Passphrases naturally result in more [failed authentication attempts](#) , are harder to remember, and as [related studies](#) show could result in more insecurities [since the end users could write them down](#) .

The single most obvious vulnerability that could undermine any encryption algorithm used, remain the use of weak passwords or passphrases. And in times when [the very same vendor](#) that's making the claims is improving the brute forcing speed through [GPU acceleration with NVIDIA cards](#) , perhaps allowing third-party password recovery software to perform better at PDF files wasn't exactly the best move in this case.

uTorrent.com hacked, serving scareware | ZDNet

The popular file sharing web sites were compromised for a brief period of a few hours, with the links to the BitTorrent client replaced by a [scareware](#) (Security Shield) download.

According to a [blog post explaining the incident](#) :

This morning on 9/13/2011 at approximately 4:20 a.m. Pacific Daylight Time (UTC -7), the uTorrent.com and BitTorrent.com Web servers were compromised. Our standard Windows software download was replaced with a type of fake antivirus “scareware” program. (UPDATE: See below for removal instructions.) Just after 6:00 a.m. Pacific time, we took the affected servers offline to neutralize the threat. Our servers are now back online and functioning normally.

Typically, when a malicious attacker gains access to such as high profile site, they would use it to spread a hacktivist message. However, the fact that the attacker had a scareware sample which would generate him revenue once it's downloaded, clearly indicates a degree of underground social networking, with uTorrent.com's attacker clearly involved in related spreading mechanisms for his scareware sample.

The sites are now clean, and are back to normal. BitTorrent.com or the BitTorrent Mainline/Chrysalis clients weren't part of the incident.

USAID.gov compromised, malware and exploits served | ZDNet

The Azerbaijan section at the United States Agency for International Development (azerbaijan.usaid.gov) has been compromised and is embedded with malware and exploits serving scripts approximately around the 1st of March. The malicious script is taking advantage of a series of redirects which are dynamically loading live exploits, or rogue security software and are all currently active. [Roger Thompson](#) at AVG Technologies [featured a video demonstrating](#) what happens when an unprotected user visits the site.

Let's dissect the attack, take into consideration the big picture, and bring a skeleton out of the closet -- one of the malware's phone back locations is a domain exclusively used by [the Russian Business Network](#) back in January, 2008.

This particular campaign relies on an embedded malicious script that appears to be dynamically creating subdomains within the cybercriminal's controlled domain. For instance, **cs.ucsb.edu.4afad2ceace1e653.should-be .cn/jan10 .cn** is where the first redirection in USAID.gov's attack takes place. From there, the surfer is taken to **orderasia .cn/index.php** and then to **orderasia .cn/iepdf.php?f=old** where the exploitation of multiple (patched) Adobe Reader and Acrobat buffer overflows takes place. Upon successful exploitation, a downloader with an [improving signatures-based detection rate](#) during the past several hours is served.

It gets even more interesting when the phone back location of the malware **fileuploader .cn/check/check.php** is revealed. The domain in question was exclusively used by [Russian Business Network/customers of the RBN](#) in January, 2008 part of the cybercrime powerhouse's attempt to throw sand in the eyes of the community by issuing fake account suspended notices whereas the malware campaigns remained active.

USAID.gov's insecurities appear to be a juicy target for cybercriminals. In 2007, the site's [Tanzanian section was hacked](#) with links redirecting to Zlob malware, followed by another research released the same year putting [USAID.gov among some of the key spam doorways](#) which WebmasterWorld analyzed back then.

Moreover, in 2007 cybercriminals indicated their ability and desire to target international governments' web sites in an attempt to use them as infection vectors in the face of such incidents as the malware embedded [French Embassy in Libya](#) ; the [Syrian Embassy in London](#) ; the [U.S Consulate in St. Petersburg](#) ; the [The Dutch Embassy in Moscow](#) ; and most recently the [Embassy of Brazil in India](#) followed by the [Embassy of India in Spain](#) - and the list is prone to expand, that's for sure.

U.K's most spammed person receives 44,000 spam emails daily | ZDNet

When you get so much spam that your anti-spam provider decides to use you in a marketing campaign, your spam

problem turns into an asset for the community, and researchers running honeypots can only envy you for the sample of spam emails you receive on a daily basis. According to [a recent press release by ClearMyMail](#) :

"ClearMyMail, has today announced the UK's Top 5 most spammed email accounts that it protects, receiving a total of 3,900 – 44,000 spam emails each day. Three of these customers have an Orange ISP and in total have around 63,339 spam emails blocked every day and 23,118,735 spam emails blocked every year.

1 – 44,001 emails blocked per day - Orange ISP 2 – 13,578 – Orange ISP 3 – 12,428 – Private domain using 123-reg/GX Networks 4 – 5,760 – Orange ISP 5 – 3,982 – Private domain using 123-reg/GX Networks

Orange customer, Colin Wells – Workshop Foreman for Stagecoach buses – has the most spammed UK inbox and ClearMyMail blocks more than 44,000 emails from entering Wells' inbox every day, amounting to around 16 million every year."

Not even [McAfee's 30 days S.P.A.M experiment](#) can come up [with such good results](#) , where 3 users receive 63,339 spam emails daily and 23,118,735 every year, mostly because these folks have been interacting with the spam messages for the past couple of years.

Typosquatting the U.S presidential election - a security risk? | ZDNet

Cybercriminals know how to take advantage of anticipated traffic by abusing the momentum of a particular event, like the

U.S presidential election in this case. Everyone, from scammers coming up with legitimately looking donation sites that they will later on spam, to the a bit more complex blackhat search engine optimization campaigns used in order to serve malware, everyone can benefit from [a typosquatted domain](#) . And what better time of the year to check whether or not domains having the potential to impersonate U.S presidential candidates are still available at the disposal of malicious parties? The same question was [asked and further investigated by Oliver Friedrichs](#) , former director of research for Symantec who recently did a study into the topic and presented his findings at this year's Black Hat con. Let's double check.

"There are about 160 different ways to type in the wrong web site for [www.barackobama.com](#) . Oliver

Friedrichs, former director of research at Symantec, knows this because he did a study of the sites that typo squat, or exploit users' misspellings of web site names to siphon off traffic from the official candidate's web site for a variety of commercial or corrupt purposes.

At [Black Hat](#) today, Friedrichs described the typosquatting study as part of a broader talk offering a warning about how any big election could be threatened by a variety of different cyber attacks. The talk is partially chronicled in a chapter that he wrote for [Crimeware](#) , a new book published by Symantec Press. Typosquatting, while interesting, is one of the smaller cyber threats. Some of the more serious ones could actually undermine confidence of voters and skew election results. Fortunately, Friedrichs said, there hasn't been a lot of use of the worst tactics yet in the current U.S. presidential campaign."

Why would a malicious party bother, and how would an opportunistic cyber criminal know when and

where to hit exactly? Because the elections engage in general, and the more people are engaged, the more people to target in general, where if even a small proportion of them fall victim into the upcoming scams it would once again be a scamming campaign worth the efforts.

According to a recently released study by the Pew Internet Project entitled "[The Internet and the 2008 election](#) ", 45% of Americans are in fact actively engaged online, potentially becoming victims of malicious campaigns taking advantage of such typosquatted domains. Some of the key findings :

- 40% of all Americans (internet users and non-users alike) have gotten news and information about this year's campaign via the internet

- 19% of Americans go online once a week or more to do something related to the campaign, and 6% go online to engage politically on a daily basis

- 23% of Americans say they receive emails urging them to support a candidate or discuss the campaign once a week or more

- 10% of Americans use email to contribute to the political debate with a similar frequency

With typosquatted domains having the potential to contribute to any successful phishing and malware campaign, what's the

current situation? A five minutes experiment I just did indicates that several hundred high quality typosquatted domains are currently available, which shouldn't come as surprise given the possibilities for abuse taking advantage of tactics such as removal of dot, missing keys, replacement by surrounding keys, reversal of keys, repetitive keys, and the possible insertion of surrounding keys in a domain name.

Rather interesting, for the time being more high quality typosquatted domains seem to have been registered for Barack Obama than for John McCain, a situation that could change pretty fast, so considering the possibilities for abuse and the fact that cybercriminals have a non-refundable donation policy, extra vigilance should be applied in the upcoming months.

Two DDoS attacks hit Network Solutions | ZDNet

Network solutions is reporting on [two consecutive DDoS attacks](#) which hit the company's networks.

According to the company, its engineers quickly took care of the issue, although some users continue reporting issues with access to web and email services:

Network Solutions experienced a distributed denial of service attack Monday afternoon, June 20, 2011 and again on Tuesday morning, June 21, 2011. Our engineers worked quickly to mitigate the attacks and services are in the process of being restored. We continue to monitor this situation, as potential risk still exists for these attacks to recur.

Last week, a [DDoS extortionist got arrested](#) for renting a botnet and attempting to blackmail German betting sites during the World Cup.

Twitter's "me too" anti-spam strategy | ZDNet

With [Twitter's continuing growth](#) , its popularity is logically starting to attract the attention of malicious parties, like

[spammers](#) , phishers, and [malware authors](#) who wouldn't mind the fact that nobody is following them when they're actively updating several hundred users with their latest propositions.

Last' week's Twitter announcement that it's "[Turning Up The Heat On Spam](#) " clearly indicates that they are not just aware of the problem, but also, admitting their current inability to deal with it the way they want to. So what is the Twitter team up to? Suspending accounts, community powered feedback on spammers accounts, and hiring dedicated personnel to look for, and shut down spammer's accounts. Will these measures work? It's all a matter of implementation, breaking out of the "me too" anti-spam strategies mentality, and listening to what the community has been saying for months.

Twitter is at least being realistic to the situation, and is not offering the Moon with these approaches :

"Suspending a spam account only works after it's already caused some damage. We have enhanced our admin tools to more accurately factor your feedback for a more timely diagnosis. When you block a spam account, we take note—when more people start blocking a spam account, we go to red alert. Blocking also puts that account out of sight and out of mind so you don't have to see it anymore.

It's unfortunate that this has to be done but we're going to hire people whose full time job will be the systematic identification and removal of spam on Twitter. These folks will work together with our support team, and our automatic spam tools. Our first "spam marshal" is starting at Twitter next week.

As always, fighting spam is a sustained activity. There is no magic wand we can wave or switch we can flip to make it all go away. Spammers will keep finding inventive new ways to advance their

motives and harm user experience and we'll keep shutting them down and slowing their progress. We just wanted to make sure everyone knows that we are taking spam seriously."

Spammers, phishers and malware authors are becoming harder to differentiate, with each and everyone of these getting involved in areas that used to be exclusively the other party's territory a while ago. Consequently, what looks like a typical phishing link, may in fact be redirecting to a live exploits page, where the typical exploits set taking advantage of the most common client-side vulnerabilities is waiting for the gullible Twitter-er. [Despite it's recent limiting of followers of a particular account to 2000](#) in order to prevent malicious users from causing more damage than they could, if Twitter really want some creative thinking applied in the process, it should consider researching what the community has already come up with in the form of tools, strategies and recommendations for Twitter to implement.

For instance, the success of the now down [Twitter Blacklist](#) was based on the simple categorization of Twitter users in

order to increase the probability of detecting a spammers account using a simple logic based on the followers and following ratio - *1:5 = twittercaster, 1:2 = notable, 1:1 socially healthy, 2:1 newbie or social climber, 5:1 twitter spammer.*

Another highly successful self-auditing service, again courtesy of the community is called [Twitter Twerp Scan](#) which *"checks the number of followers of everyone on your contact list, the number of people they are following, and the ratio between those. If the person is following more than (n) people (can be customised), and has a Following-to-Followers ratio higher than 1:(m) (can be customised), you'll be notified by a link. "*

There's also never been a shortage of pragmatic solutions to at least make it harder to spammers to efficiently spam the network, with [tips and recommendations](#) made by Twitter users a couple of months ago :

[Add Followers/Following metrics and Follow/Block buttons to New Follower email](#) ["Report Spam" links need to be placed on user page](#) [Require captcha on Follow](#) [Analyze New Followers feature](#) [Ban](#)

[URL's for repeat spam offenders](#) [Twitter spam mitigation via SURBL applied to young](#) [Follow ratio inequity accounts](#)

Twitter's successful anti-spam strategy lies within whether or not they will consider the know-how and experience offered by the community, which as always finds its ways to adapt to a specific situation long before a service has come to introduce its own solution.

Add spam button courtesy of [chadspacey's photostream](#) .

Twitter worm author gets a job at exqSoft Solutions | ZDNet

UPDATE : [Mikeyy Mooney of Stalk Daily gets Hacked](#) . Here's [more info](#) .

Now that was so fast that even [Owen Thor Walker](#) (AKILL) and [Michael Calce](#) ([Mafiaboy](#)) should envy the short cybercrime-to-job offer cycle here. 17 years old [Mikeyy Mooney](#) , the author/spreader of [StalkDaily/Mickeyy XSS worm](#) that exploited Twitter through trivial web application vulnerabilities during the weekend, has landed a job as a web applications developer at [exqSoft Solutions](#) .

Do you fancy him? [I don't, and so do others](#) . Here's why you shouldn't, as well as the implications of what is slowly becoming a dangerous trend.

Imagine the villains vs cybercrime task force, an internationally recognized team including [Romanian phishers](#), [ex-carding kings now politicians](#) , initiators of the [first major DDoS attack](#) that hit the most popular web sites in 2000 (including ZDNet) and who else are we missing? Oh yeah, the [Pinch malware authors](#) , but "sadly" they're in jail.

Cutting the sarcasm, this most recent hire indicates an emerging trend and sends a wrong signal. Namely, that conducting unethical pen-testing against a top web property's web applications in order to put the proof of concept code into action by launching a worm in order to prove the obvious, can indeed land you a job offer. A similar case happened in July, 2008, when a [XSS worm at Justin.tv infected 2,525 profiles in order to prove the obvious](#) - the site's "wormability". Back then I pointed out the same concern :

Now, [proof of concept of what exactly](#) remains questionable, since [if the research community was to exploit](#) every site [vulnerable to SQL injections](#) or [high profile sites vulnerable to critical XSS flaws](#) , in order to embed a counter within and then come up with fancy graphs saying this is the number of people that could have been

affected by this flaw, we would be dealing with more PoCs next to the real security incidents executed by malicious parties.

It's important to point out that exqSoft Solutions appears to be fully aware of the basics of guerrilla PR campaigns. The company established in 2000 is nowhere to be found in the public space, that's of course until it hires [Mikeyy Mooney](#) to make a mainstream media appearance for the very first time.

Who's next on the hiring spree? From a web application security perspective, that could easily be the [Asprox botnet](#) authors, having [SQL injected](#) over 1.5 million pages ([500,000 sites](#)), making Mikeyy's XSS worm look like a bit of a shy one.

Twitter hit by multiple variants of XSS worm | ZDNet

During [the weekend](#) and early [Monday](#) , at least four [separate](#) variants of the original StalkDaily.com XSS worm hit the popular micro-blogging site Twitter, automatically hijacking accounts and advertising the author's web site by posting tweets on behalf of the account holders, by exploiting cross site scripting flaws at the site.

17 years old author of the worm [Mikey Mooney claimed responsibility for the worm](#) (photo of him is available, [podcast interview](#) as well) citing boredom, and insisting that the most [recent variant launched on Monday](#) aimed to prove that Twitter did not fix the cross site scripting flaw which [they claim was already taken care of](#) earlier during the day.

Let's analyze all of Mikey's campaigns.

With the proof of concept code for both of the worms now publicly available, and with [NoScript's creator Giorgio Maone logical conclusion](#) that Twitter may have in fact not taken care of the XSS flaw as the second variant launched by a third-party was a basically obfuscated version of the first one, Mikey's claims may in fact be true.

The original StalkDaily.com/Mikeyy XSS worm campaign was using automatically Tweeting the following messages:

"Dude, www.StalkDaily.com is awesome. What's the fuss?" "Join www.StalkDaily.com everyone!" "Woooo, www.StalkDaily.com :)" "Virus!? What? www.StalkDaily.com is legit!" "Wow...www.StalkDaily.com" "@twitter www.StalkDaily.com"

Mikey's first release would then attempt to steal cookies and continue spreading by accessing the following URLs - **mikeyyloolz.uuuq.com/x.js** and **mikeyyloolz.uuuq.com/x.php** which he has already removed.

The second Mikeyy XSS worm launched on Sunday is a bit more interesting as it appears that this is a copycat worm which used to

take advantage of the following messages:

"Wow...Mikeyy." "Man, Twitter can't fix shit. Mikeyy owns. :)" "Dude! Mikeyy! Seriously? Haha. ;)" "Dude, Mikeyy is the shit! :)" "damn mikeyy. haha." "Twitter should really fix this..." "Mikeyy I am done..." "Mikeyy is done.." "Twitter please fix this, regards Mikeyy"

The second variant -- including a modified version of it -- would then attempt to further propagate by directing the affected users to the following URLs - **content.ireel .com/jsxss.js** ; **content.ireel .com/xssjs.js** ; **omghax.uuuq .com/x.php** ; **omghax.uuuq .com/woo.php** ; **bambamyo.110mb .com/wompwomp.js** . What we've also got here is an indication of a compromise at iReel.com.

The most recent variant of the worm was launched yesterday, and was apparently relying on the exploitation of an input validation flaw in what Mikeyy claims to be a second vulnerability that he exploited at Twitter.

Go through related incidents: [Commercial Twitter spamming tool hits the market](#) ; [XSS worm at Justin.tv infects 2,525 profiles](#) ; [Four XSS flaws hit Facebook](#) ; [Facebook vulnerable to critical XSS, could lead to malware attacks](#) ; [HSBC sites vulnerable to XSS flaws, could aid phishing attacks](#) ; [Google fixes critical XSS vulnerability](#).

The campaign was using the following messages to propagate:

"Twitter, freaking fix this already. >:[- Mikeyy" "Twitter, your community is going to be mad at you... - Mikeyy" "This worm is getting out of hand Twitter. - Mikeyy" "RT!! 4th gen #Mikeyy worm on the loose! Click here to protect yourself: <http://tinyurl.com/cojc6s>" "This is all Twitters fault! Don't blame Mikeyy!!" "ALERT!! 4TH GEN MIKEYY WORM, USE NOSCRIPT: <http://bit.ly/4ywBID>" "How TO remove new Mikeyy worm! RT!! <http://bit.ly/yCL1s>"

Deobfuscated the scripts directs to **twitter .com/reberbrerber** and to **stalkdaily .com/ajax.js** . Interestingly, based on the public stats from **bit.ly** , we can easily evaluate the click-through rate of the latest campaign, with [20,140 clicks so far](#) , with 9,268 from the U.S followed by 3,039 from the U.K for the first URL, and [8,961 clicks](#) , with 4,095 from the U.S, followed by 1,452 from the U.K. for the second one.

With or without the malicious intent of spreading malware, Mikey's persistent actions aiming to prove Twitter's inability to fix the cross site scripting flaws are illegal, and so is the potential compromise of iReel.com for hosting purposes of the javascript code. And whereas these campaigns did not introduce malware or tried to monetize the traffic by for instance installing scareware, different people have different motivations, so instead of waiting for the hardcore cybercriminals to take advantage of such flaws, Twitter should really start treating (trivial) cross site scripting flaws more proactively.

Twitter hacked, 250,000 users affected | ZDNet

Twitter has just reported that earlier this week, it was [a victim of a successful compromise of its systems](#), resulting in the "limited access" to user information, including usernames, email addresses, session tokens, and encrypted/salted passwords, affecting approximately 250,000 users.

More details:

This week, we detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users. As a precautionary security measure, we have reset passwords and revoked session tokens for these accounts. If your account was one of them, you will have recently received (or will shortly) an email from us at the address associated with your Twitter account notifying you that you will need to create a new password. Your old password will not work when you try to log in to Twitter.

According to [Bob Lord](#), Twitter's Director of Information Security, the attack was the work of professionals, and Twitter is actively cooperating with law enforcement in an attempt to prevent further damage caused by these attackers.

What can you do to protect your Twitter account? Ensure that in case you receive a password-reset email from Twitter, it indeed points to Twitter's domain, as opportunistic cybercriminals could easily start impersonating Twitter, and mass mail millions of emails in an attempt to gain access to your account. If you do receive a password-reset email from Twitter, ensure that you're using a strong password, and that you've changed it from a malware-free host.

Find out more about Dancho Danchev at his [LinkedIn profile](#).

Trusteer launches search engine for malware configuration files | ZDNet

Trusteer's recently launched "[Attack Trace](#)" search engine aims to help financial institution by letting them search through the configuration files of popular banker malware SilentBanker, WSNPOEM/Zeus/PRG/Zbot and Torpig in order for them to verify whether or not their sites are targeted. And while the search engine is a marketable way to initiate a response channel, it doesn't take into consideration a simple fact - that modern banker malware is no longer exclusively targeting a particular E-banking site, but is [targeting all of them simultaneously](#).

"The Trusteer Attack Trace search engine allows IT professionals to submit their organization's web address and see a list of malware configuration files that are designed to commit fraud against their brand. By typing their URL address into the Attack Trace search engine, users get a glimpse into the cross section of malware that is specifically aimed at their website and what the code is written to accomplish. The Trusteer Attack Trace search engine searches for leading Trojans and other attack codes including Torpig/Sinowal, WSNPOEM, and NetHell."

Doing a [basic search for https sites](#), you'll notice the obvious fact that the majority of popular E-banking and online payment services are well researched, and already targeted. The mindset of the crimeware author is fairly simple and that's what makes it so dangerous since it relies on two key objectives - scalability and efficiency. Due to the modular nature of modern crimeware, as well as the fact that its open source, the original author or the crimeware kit's users are capable of writing their own "injects" which basically represent researched session activities at targeted financial institutions, thereby making the process of hijacking it efficient.

If financial institutions really want to find out whether they're targeted by modern banker malware, they should automatically assume so without any hesitation.

TROYAK-AS: the cybercrime-friendly ISP that just won't go away | ZDNet

Over the past week, security researchers and vendors have been playing a cat-and-mouse game with a [cybercrime-friendly ISP known as TROYAK-AS](#) , one of the key "phone back" locations for the command and control servers for the [Zeus crimeware](#) serving campaigns for Q1, 2010.

The results so far? A series of attempts by the cybercriminals to restore access to their botnet, and an invaluable learning experience for the community, with the gang exposing node after node of malicious activity.

Why is TROYAK-AS's take down so important at the bottom line?

Disrupting the ISPs activities doesn't mean that the remaining and currently active Zeus campaigns would be somehow disrupted. This common misunderstanding stems from the Zeus crimeware wrongly perceived as a botnet similar to, for instance, the Conficker botnet. In comparison, [Zeus is a DIY crimeware](#) -- also available as [a managed crimeware service since 2008](#) , perhaps even earlier -- with an unknown of cybercriminals operating their own Zeus botnets.

Taking it down means undermining the effectiveness of a huge percentage of their campaigns launched during the first quarter of the year. Not only does this mean disruption of their operations, but most importantly, loss of confidence on behalf of their customers in [TROYAK-AS's](#) ability to stay online.

Go through analysis of Zeus crimeware serving campaigns using TROYAK-AS's services for Q1, 2010 : [Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware](#) ; [Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams](#) ; [PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild](#) ; [Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild](#) ; [Keeping Money Mule Recruiters on a Short Leash - Part Two](#)

Ironically, a representative from TROYAK-AS's, your typical cybercrime-friendly virtual neighborhood, is doing his best to retain their underground reputation, by attributing the shut down to the fact that they forgot to pay their upstream provider. Moreover, [Roman Starchenko's comments](#) -- fake name that's for sure -- demonstrate the harsh reality in respect to fighting cybercrime internationally, in particular the lack of cooperative efforts into going after the people, not the networks:

"I know, some of [the] clients of our service might be used for something you called 'botnet'. Anyway, we did not receive any letter from any officials of our country, so will not perform any actions as our law said. "

As of Wednesday, March 10th, 2010, TROYAK-AS made multiple attempts to find an upstream provider, temporarily relying on the following ones:

AS44051 - YA-AS Professional Communication Systems
AS8342 - RTCOMM-AS RTComm.RU Autonomous System
AS25189 - NLINE-AS JSC Nline AS12993 - DEAC-AS

Today, [TROYAK-AS is "de-peered"](#) again. However, contingency planning is clearly part of the provider's quality assurance process, especially in times when the days of the "sitting duck" cybercrime-friendly ISPs are nearly over.

What are TROYAK-AS's customers up to?

Clearly, some of them have lost confidence in TROYAK-AS's ability to remain online, and on Friday, March 12th, 2010, resumes their malicious operations by launching another campaign - "[Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild](#)". In reality, their customers have a pretty diverse choice of providers offering services similar to those of TROYAK-AS, with cybercriminals offering a mix of legitimate and purely malicious infrastructure for anything cybercrime related.

Go through related posts on previously shut down cybercrime-friendly ISPs : [With or without McColo, spam volume increasing again](#) ; [Atrivo/Inter cage's disconnection briefly disrupts spam levels](#) ; [Google: Spam volume for Q1 back to pre-McColo](#)

[levels](#) ; [Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown](#)

TROYAK-AS remains "de-peered". It's only a matter of time before they find another upstream provider. [The ISP remains the tip of the iceberg](#) , with Russia, followed by China and the U.S listed as the top Zeus malware hosting countries.

What the cybercriminals are forgetting, is the fact that every time they attempt to obtain access to the botnets, they sacrifice their [OPSEC \(operational security\)](#) . Sooner or later, the analysis of their activities would move beyond the WHOIS records, and start profiling them on first name basis.

UPDATE, Wednesday, March 17, 2010: Today, the folks at RSA FraudAction Research Lab posted an update "[AS-Troyak Exposes a Large Cybercrime Infrastructure](#) ", offering an insight into the infrastructure that the cybercriminals exposed on their way to put AS-TROYAK back online.

What do you think? Are such take downs relevant in the long-term, or is the "learning experience" gained worth the efforts? Does it really matter if a particular botnet gets shut down, given the fact that the botnet masters remain at large, and would basically aggregate a new one?

TalkBack.

Trojan exploiting unpatched Mac OS X vulnerability in the wild | ZDNet

The source code of a trojan horse exploiting last week's uncovered [local root escalation vulnerability](#) in Mac OS X 10.4 and

10.5 has been released in the wild, allowing malicious attackers to take advantage of the ARDAgent-based trojan in what appears to be a very short vulnerability-to-malware cycle, since the trojan template was released on the same day as details for the vulnerability emerged.

Discussion and release of the source code originally took place at the [Mac Shadows forums](#) , whereas the source code is now circulating across many other forums and IRC chat rooms, including several popular ones mainly visited by Chinese script kiddies.

According to [an advisory](#) issued by [SecureMac](#) last week :

SecureMac has discovered multiple variants of a new Trojan horse in the wild that affects Mac OS X 10.4 and 10.5. The Trojan horse is currently being distributed from a hacker website, where discussion has taken place on distributing the Trojan horse through iChat and Limewire. The source code for the Trojan horse has been distributed, indicating an increased probability of future variants of the Trojan horse.

The Trojan horse runs hidden on the system, and allows a malicious user complete remote access to the system, can transmit system and user passwords, and can avoid detection by opening ports in the firewall and turning off system logging. Additionally, the AppleScript.THT Trojan horse can log keystrokes, take pictures with the built-in Apple iSight camera, take screenshots, and turn on file sharing. The Trojan horse exploits a recently discovered vulnerability with the Apple Remote Desktop Agent, which allows it to run as root.

Compared to this week's reported [PokerStealer trojan horse targeting Mac OS X](#) users, by trying to trick them into

empowering the malware with administrator capabilities, the ARDAgent-based trojan is doing it automatically, unless of course [you've already taken care of the issue](#) until a fix for it is officially available.

The author of the trojan, Adrew, even left a copyright notice within, however, it appears that the source code for the trojan isn't a one-man operation, but the result of a collaborative discussion aiming to add as many modules as possible. Here's [what he thinks of OS X security](#) , according to his own statement :

"Apple tells us that OS X is safe and secure and fails to actually confirm that it is so on their own. We are left to experiment and test our own security and too often we discover that we aren't actually as secure as we were led to believe," Andrew said in an e-mail. "When you are seeking information about how to secure your own system, frequently the best sources of that information are hackers, not the vendors."

Going full-disclosure with the idea to shorten the time until a patch is released by the vendor for the sake of closing the "window of opportunity" for malicious abuse of the vulnerability is one thing, releasing a do-it-yourself trojan template in a vulnerability-to-malware fashion is entirely another.

Trivial security flaw in popular iPhone app leads to privacy leak | ZDNet

A trivial security flaw within a popular [photo sharing iPhone app known as Quip](#) , has exposed thousands of shared photos, with repositories of them -- including the naked ones -- already circulating across the Web.

[Addy Mobile, Inc](#) , the company behind the application, is coming under harsh criticism due the fact that the flaw and its active exploitation has been known for a few months, possibly longer, with no actions taken to ensure that it can no longer be abused.

[More details on the flaw](#) , including a statement from Quip's founder:

Basically, every time someone is sharing a photo, it's uploaded on Quip's web server using just 5 random letters and digits for generating the URL, allowing a potentially malicious user to use brute force and obtain private photos exchanged between Quip's users with no technical sophistication.

Moreover, not only were the URLs easy to brute force, but also, the URLs weren't even instructing search engine crawlers to skip them, resulting in a small number of them appearing in Google's index.

The founder of the company issued the following statement in response to the flaw:

"Hello, this is Ish, the founder of Addy Mobile, makers of the Quip app. As soon as this post came to our attention, we immediately shut down our servers. We have also now disabled all S3 access and have started to systematically secure all files in the system. We will not bring the system back up until we have adequate security around all files shared over Quip. I apologize to our users for this security breach and promise we will do everything in our power to make sure none of their information is exposed once we bring the service back up. The vision for Quip has always been to provide users a quick, simple, and affordable way for iPhone users to send picture

messages without paying exorbitant carrier fees. We are a small company (3 people) but we will work as quickly as possible to bring back the service up in a safe and secure manner."

According to [Quip's description](#) , millions of people have already shared photos using the service. [Quip's server](#) is currently offline.

Transmitter.C mobile malware spreading in the wild | ZDNet

Researchers from [NetQin Tech.](#) are reporting on a newly discovered mobile malware variant ([Transmitter.C](#)) distributed through a modified version of legitimate mobile application. Upon execution, the malware attempts to automatically spread by SMS-ing hundreds of messages linking to a web site where a copy of it (**sexySpace.sisx**) can be found.

NetQuin's CEO, Dr. Lin Yu provides more insight into the nature of the malware, its financial implications for the infected user, as well as thoughts on the future of mobile malware.

Go through the Q&A.

Dancho : What are some of the characteristics of Transmitter.C?

Dr. Lin Yu : As a foreign variant of previous erotic short message virus (Transmitter.A), this virus camouflages in a normal third party mobile phone software " Advanced device locks" to inveigle the users to install it.

After installation, this virus will be automatically started up. Just a minute, it will automatically access network for about 3 minutes. Later, this virus will send short messages externally at interval of 10 - 15 seconds. As can be observed from the communication record, there are large amount of records of sending short messages, all the numbers to which short messages are sent are strange numbers, but it is completely impossible to find the record of short messages that have been sent in the Sent Box.

After having sent about 500 strange short messages, this virus will traverse the cards folder to send out short messages. Furthermore, this virus can automatically identify mobile phone languages and send different short message contents including "*Classic Gongfu stories , City passion , Wife change , School girl , Violent incest ... Please immediately access? " A very interesting girl . Try it now! "* etc., and attach a URL after each short message.

This virus will run away with user's tariff by sending out short messages at such high frequency. In addition, it is very likely that this virus forcibly subscribes some services for the users, thus consuming user's tariff.

Furthermore, this virus has transmissibility. In the form of obscene short messages, it will inveigle the users to click the links in the contents of short messages. Upon clicking such links, a user will download virus to his/her mobile phone, becoming the next virus-spreader. In addition, this virus can also be transmitted in the form of legitimate third party software that is put in the Website and Forum for downloading mobile phone software.

Go through related mobile malware posts: [Attacks on NFC mobile phones demonstrated](#) ; [New mobile malware silently transfers account credit](#) ; [New Symbian-based mobile worm circulating in the wild](#)

Dancho : How is Transmitter.C different than any other Symbian malware?

Dr. Lin Yu : As compared with the Symbian malicious software formerly discovered, Transmitter.C has even stronger transmissibility and harmfulness: It not only has the corresponding server end for coordination, but can also be dynamically adapted to the current language of mobile phone and thus send short messages to address lists and strange numbers in different languages. Furthermore, utilizing obscene short messages with links, it can inveigle the users to click it for installation. If this virus has been transmitted to mobile phones, it will bring tremendous economic loss and reputation crisis to the users.

[Next](#) -->

Dancho : Since the application mentioned as the propagation vector for the malware -- Advanced Device Locks -- is a legitimate one, is this a case where a legitimate software has been brandjacked and modified in order to trick users into installing it?

Dr. Lin Yu : Yes. This virus can camouflage as legitimate software for transmission. Camouflage mode: The executable body of virus attaches at normal software to inveigle the users to install it.

Dancho : Are the malware authors attempting to somehow monetize the campaign and earn profit in the process, or is Transmitter.C basically a proof of concept that can only result in huge phone bills due to the short time interval between sending the SMS messages?

Dr. Lin Yu : This malicious software is designed to realize the object of making commercial profit. Transmitter.C has promoted some malicious links. Very likely, it forcibly subscribes some services for the users, thus consuming the tariff of users; These malicious links may induce a user to download virus to his/her mobile phone, so that this user will become the next virus-spreader.

Dancho : How would you describe the current state of mobile malware? Is the inevitable growth of the micro-payment market prone to increase cybercriminal's interest in mobile malware, or would they go after the intellectual property data stored on the smart devices?

Dr. Lin Yu : These two aspects will become the major targets attacked by mobile phone malicious software.

In our opinion, with the intellectualization of mobile phones and the increase in network bandwidth, there will be more and more mobile phone malicious software and their routes of transmission. Furthermore, because many users have get accustomed to saving their privacy information such as bank account, address list and photograph and their mobile phones have payment function, the mobile phone malicious software will generate much more hazards than computer malicious software.

According to the study on the viruses we have captured, most of mobile phone malicious software are still mainly designed to consume the tariff of users by means of automatic networking and automatic transmission of malicious short messages for fee reduction. In addition, few malicious software have turned to steal the privacy information of users. In particular, the privacy information in the users' mobile phones (short message, address list and picture etc.) will become the main targets of attack by malicious software and will be likely transmitted in the modes of short messages and networking, resulting in the disclosure of user's privacy.

Tracking down the Storm Worm malware | ZDNet

What is the current state of Storm Worm activity, how many infected IPs are found to host the malware on a daily basis, which are the latest domains used by the Storm Worm, and which countries have the largest infected population? You can easily find that out, if you keep an eye on TrustedSource's Storm Tracker, a handy tool providing both, researchers and end users with a real-time overview of the current Storm Worm activity, of course, based on a single vendor's sensor network as a sample of malicious activity. What are some of the categories monitored by the service?

[TrustedSource's Storm Tracker](#) monitors the following categories :

- Daily New Web Proxy IPs - Most Active Storm Web Proxy IPs - Top Storm Domains - Newly Activated Storm Web Proxy IPs - Recently Seen Storm Web Proxy IPs - Geolocation of Storm Web Proxy IPs

After taking credit for the pioneering of P2P botnet command and control, next to the rest of [commonly used botnet communication platforms](#) , as well as [the fast-fluxed botnet structure](#) in order to create a [dynamic and harder to shut down botnet](#) , Storm Worm is currently in the orienting process if we're to consider [the OODA loop](#) . What does this mean? It means that, for instance, once observing the success rate of the recent [SQL injection attacks](#) , the botnet masters decided to enjoy all the noise generated by the copycats, [reintroduce the same tactic](#) that they were using in August, 2007, and started [injecting their exploit serving domains](#) into vulnerable sites hoping they would go unnoticed in between the rest of the currently active SQL injection campaigns.

Considering Storm Worm's historical pattern of utilizing [event-based social-engineering campaigns](#) , and periods of passive behaviour, once the botnet masters orient and decide, they'll act again for sure. It's always calm before the real storm, especially in times when [multiple storms are fighting for market share](#) , isn't it?

Top ten worst spam registrars notified by ICANN | ZDNet

In a reponse to the [recently released](#) cluster analysis of the [top 10 worst domain registrars](#) in terms of spam and junk content hosting domains, the [ICANN has taken steps](#) to approach the non-compliant registrars :

More than half of those registrars named had already been contacted by ICANN prior to publication of KnujOn's report, and the remainder have since been notified following an analysis of other sources of data, including ICANN's internal database. With tens of millions of domain names in existence, and tens of thousands changing hands each day, ICANN relies upon the wider Internet community to report and review what it believes to be inaccurate registration data for individual domains. To this end, a dedicated online system called the Whois Data Problem Report System ("WDPRS") was developed in 2002 to receive and track such complaints. ICANN sends, on average, over 75 enforcement notices per month following complaints from the community. We also conduct compliance audits to determine whether accredited registrars and registries are adhering to their contractual obligations," explained Stacy Burnette, Director of Compliance at ICANN. "Infringing domain names are locked and websites removed every week through this system."

And while it the data speaks for itself, the issue of responsibility-forwarding is a bit more complex than it seems, allowing certain observations in the cluster analysis to be easily re-engineered.

For instance, the first registrar with the highest illicit score, has a total of 897,962 domain names, where the 15,551 spam domains registered through it were found in 1,644,986 spam messages featuring the domains. Hypothetically, if I were a spammer, I can superficially engineer the top ten worst domain registrars if I purchase a couple of hundred recently dropped domain names historically registered through a specific registrar, launch a massive

spam campaign and send out 5 million messages to increase the bad reputation of the registrar whose historical registration services I'm abusing. The results would vary based on the number of spam messages sent, and the domain name registrar that would pop-up as having registered the highest proportion of the dropped or deleted domain names that I've recently purchases on a volume-basis, without even bothering to see who's the registrar.

Furthermore, excluding the more [pragmatic abuse of domain names](#) in the face of [typosquatting](#) and [cybersquatting](#) next to illicit domain registration, I find the idea of intentionally registering a domain to be used for hosting of a spam site, a very Web 1.0 one. Just like the domain name registrars who emphasize on efficiency, and therefore violate ICANN's compliance practices, spammers and scammers are also interested in efficiently obtaining as many domain names as possible, this is where the dropped or deleted domains services come into play in their full Web 2.0 capacity, with several of these offering purchases on a volume basis with the idea that the more domains you purchase, the less you'll pay for them. And with the transparency build by these services, there are proprietary domain portfolio management tools created intentionally for the purpose of mass-registrations and management of such domain farms. Therefore, I think the emphasis should be put on who's been hosting the spam/scam domain and proving the malicious parties with stable uptime for a given period of time, and which are the registrars lacking any [brandjacking monitoring capabilities](#) , compared to assessing which registrar's services were used to register the domain that was later one used for malicious purposes. Otherwise, we're shifting the discussion to the point where're we'll argue which top level domain name is the most malicious one, where clustering is also possible with [CNNIC's .CN domain name for one yuan campaign](#) which already resulted in 8.4 million .CN registered (bogus) domain names.

Today's assignment : Coding an undetectable malware | ZDNet

Today's dynamic Internet threatscape is changing so rapidly, that the innovations and creativity applied by malware

authors can easily render an information security course's curricular on malware outdated pretty fast, or worse, provide the students with a false feeling of situational awareness about today's malware that's driving the entire cybercrime ecosystem at the end of the day. In fact, one can easily spot an outdated academic curricular on the basis of the malware it's discussing, and whether or not the lecturer is even bothering to imply that antivirus software the way it is, and the way it's been for the past couple of years, is only mitigating a certain percentage of the threat, next to eliminating it entirely and urging everyone to "keep their antivirus software up to date."

George Ledin, a professor at Sonoma State University thinks that coding malware helps students better understand the enemy. [What is Ledin trying to achieve anyway?](#)

"Ledin insists that his students mean no harm, and can't cause any because they work in the computer equivalent of biohazard suits: closed networks from which viruses can't escape. Rather, he's trying to teach students to think like hackers so they can devise antidotes. "Unlike biological viruses, computer viruses are written by a programmer. We want to get into the mindset: how do people learn how to do this?" says Ledin, who was born to Russian parents in Venezuela and trained as a biologist before coming to the United States and getting into computer science. "You can't really have a defense plan if you don't know what the other guy's offense is," says Lincoln Peters, a former Ledin student who now consults for a government defense agency."

To code an undetectable malware in an academic environment in order to scientifically prove that signatures based malware scanning wouldn't detect the just coded malware, or to keeping providing a

false feeling of security by the wrongly positioned antivirus software? That's the question Sonoma State University's George Ledin seems to be asking, and he's naturally receiving a lot of criticism from companies "making their living fighting viruses" reaching such heights as companies speculating on not hiring his students, now capable of coding malware. The companies however, forget one thing - how easy is in fact to "generate" an undetectable piece of malware using the hundreds of malware builders that they are aware of, ones that come very handy for internal benchmarking purposes for instance.

For the past couple of years, antivirus software has been a pure reactive security solution, namely compared to pro-active

approaches embraced by the vendors who are in catch-up mode with the malware authors, it was reacting to known threats. Two months ago, [Eva Chen, Trend Micro's CEO made some very bold, but pretty realistic statements](#) on signatures based malware scanning, and how the entire industry was wrongly positioned for the past 20 years :

"In the antivirus business, we have been lying to customers for 20 years. People thought that virus protection protected them, but we can never block all viruses. Antivirus refresh used to be every 24 hours. People would usually get infected in that time and the industry would clean them up with a new pattern file. In the last 20 years, we have been misrepresenting ourselves. No-one is able to detect five and a half million viruses. Nowadays there are no mass virus outbreaks; [malware] is targeted. But, if there are no virus samples submitted, there's no way to detect them."

Precisely, so what Ledin is blamed for is in fact an outdated fact by itself starting from the basic nature of how antivirus software works. [The very same outdated approach of proving a known fact](#) will be taken by the upcoming ["The Race to Zero" undetectable malware coding contest](#) to be held at this year's Defcon security conference. Moreover, in between [vendors counting how much malware they are detecting](#) , taking a peek at publicly obtainable [statistics on detection rates for malware in the wild](#) , you will see how dynamic "the best antivirus software" position is, since it literally changes every day.

And theoretically, even "the best antivirus software" wouldn't be able to detect the malware coded by Ledin's students, or the one that [someone requested to be coded for hire](#) , a service that's been getting increasingly popular these days due to its customerization approach.

Ironically, the IT underground is a step ahead of George Ledin, using distance learning approaches by including video

tutorials on how to use malware kit, including practical examples of successful attacks and providing tips from personal experience while using it. Coding an undetectable malware in 2008 isn't rocket-science, with do-it-yourself malware builders providing point'n'click features integration that used to be only available to a sophisticated malware author a couple of years ago. Then again, having an undetected malware, doesn't mean that they'll be able to successfully spread it and infect millions of users, so from a strategic perspective it's all about the tactics and combination of tactics that would use in their campaign.

[Before you judge Ledin's vision](#) , ask yourself the following - does coding malware ultimately improve the career competitiveness of his students in the long-term, or isn't what he's trying to prove a known fact already?

Related posts:

[The Neosploit cybercrime group abandons its web malware exploitation kit](#) [Storm Worm's Independence Day campaign](#) [Storm Worm says the U.S have invaded Iran](#) [200,000 sites spreading web malware](#), [China's hosting the most](#) [Who's behind the GPcode ransomware?](#) [Trojan exploiting unpatched Mac OS X vulnerability in the wild](#)

Thousands of web sites compromised, redirect to scareware | ZDNet

Updated: Thursday, November 19 - [According to eSoft](#) who contacted me, they've been [monitoring the campaign since September](#) , with another 720,000 affected sites back then.

There are now over a million affected sites serving [scareware](#) , with only a small percentage of them currently [marked as harmful](#) . Google has been notified. As always, [NoScript](#) and your [decent situational awareness](#) are your best friends.

Security researchers have detected [a massive blackhat SEO \(search engine optimization\) campaign](#) consisting of over 200,000 compromised web sites, all redirecting to fake security software ([Inst_58s6.exe](#)), commonly referred to as [scareware](#) .

More details on the campaign:

The compromised sites are hosting legitimately looking templates, using automatically generated bogus content, with a tiny **css.js** ([Trojan-Downloader.JS.FraudLoad](#)) uploaded on each of them which triggers the scareware campaign only if the visitor is coming a search engine listed as known http referrer by the gang - in this case Google, Yahoo, Live, Altavista, and Baidu :

"Cyveillance has discovered a complex attack vector that uses Google search results to distribute malicious software (malware) to unsuspecting Internet users. Using this attack vector, users click on links within Google search results and are routed to sites that attempt to download malware to their computers. The attack method also relies on inattentive webmasters who do not update the software on their sites and often unknowingly provide the material that appears in the search results.

The common string albums/bsblog/category is found in the URLs for all these blogs. By simply using the Google search parameter allinurl, along, you can see how many other sites contain the same string. As can be seen in the image above, more than 260,000 URLs

are presented in Google's search index leading to blogs similar to the ones illustrated in our example.

As you can see, only a small portion of sites in the search results carry a warning provided by Google. The reason for the small number of warnings is likely because the actual attacks do not take place on the website URLs in the search results, but on the sites you're redirected to thereby decreasing the chances that Google will designate the destination sites as harmful."

At first, it would appear that the campaign is an isolated one and is maintained by a cybercrime enterprise yet to be analyzed. However, analyzing it reveals a rather anticipated connection - [the massive blackat SEO campaign](#) has been launched by the same people who operate/or manage the campaigns for the Koobface botnet. For instance, the domains mentioned by Cyveillance, as well as the newly introduced ones over the past couple of hours, are [the very same domains currently embedded on Koobface infected hosts](#) .

Go through related posts - [The ultimate guide to scareware protection](#) ; [My scareware night and how McAfee lost a customer](#) ; [Scareware scammers hijack Twitter trending topics](#) ; [9/11 related keywords hijacked to serve scareware](#) ; [Koobface Botnet's Scareware Business Model - Part One](#) ; [Koobface Botnet's Scareware Business Model - Part Two](#)

How did they manage to compromise the sites? Through web application vulnerabilities as the attack vector, with [OWASP's recently updated Top 10 most critical web application security risks](#) , highlighting some of the riskiest ones.

Thousands of legitimate sites SQL injected to serve IE exploit | ZDNet

Once again confirming the trend of having more legitimate sites serving exploits and malware than purely malicious ones, Chinese hackers have been [keeping themselves busy](#) during the last couple of days, [launching massive SQL injection attacks affecting over 100,000 web sites](#) .

The [SQL injection attacks](#) serving the [just patched Internet Explorer XML parsing exploit](#) , are launched by several different Chinese hacking groups, and with several exceptions, are primarily targeting Asian countries which is a pretty logical move given the fact that it's a password stealing malware for online games that is served at the bottom line.

Which is the most targeted country?

According to some stats from Symantec, China ironically remains the most actively targeted country by the IE exploit, ironically in the sense that it was Chinese researchers that leaked the exploit at the first place. Moreover, the 100,000 web sites cited as being infected by Symantec, should be taken as a very conservative metric, since more domains are being injected and as previous campaigns, the number of affected sites could change pretty fast.

Consider for a while the big picture. With or without a patch for the IE exploit, committing cybercrime through the exploitation of already patched client-side vulnerabilities would continue growing - it has been throughout the entire 2008. Despite being old-fashioned compared to Russian cybercriminals that would have included the exploit within their [web malware exploitation kits](#) and started serving banker malware instead of password stealing malware, the Chinese attackers appear to be well aware of this trend, and therefore all of the IE exploit serving sites are also serving several other exploits targeting Adobe's Flash, Acrobat Reader and RealPlayer for starters.

Recent studies continue emphasizing on the fact that [millions of users not only continue browsing the web using insecure browsers](#) ,

but also, are so browser vulnerabilities centered and they [ignore the rest of the software](#) running on their PCs as a [potential infection vector given they're running an insecure versions of it](#) - and yes they are. Cybercriminals are aware of this insecure Internet browsing, and are therefore including [sets of exploits](#) targeting each and every [version known to be vulnerable](#) of a particular software in order to [increase the chances for a successful infection](#) . This particular SQL injection attack is the most recent example of this mentality.

In 2008, cybercriminals continue infecting thousands of new hosts on daily basis using 2007's critical vulnerabilities, because instead of patching vulnerable software, the majority of end users remain comfortable with their [false feeling of security](#) .

Thousands of Israeli web sites under attack | ZDNet

In the wake of the escalating conflict between Israel and Hamas, it didn't take long before pro-Hamas supporters organized themselves and started to [defacing thousands of pro-Israeli web sites](#) in order to use them as vehicles for propaganda -- Israel is meanwhile [hijacking TV signals](#) .

For the time being, pro-Israeli sites remain automatically probed for web application vulnerabilities through search engines reconnaissance of the Israeli web space by **JURM-TEAM** and **TEAM-Evil** , two groups [working together and using identical templates for the defaced sites](#) .

Compared to previous hacktivism ([politically motivated hacking](#)) activities on behalf of this group consisting primarily of mass web site defacements through web applications vulnerabilities exploitation, last week TEAM-Evil managed to hijack the DNS records of several hundred Israeli domains -- [traffic was redirected to bestsecurity.jp](#) -- once [compromising the administration panel of the domain registrar DomainTheNet](#) .

(Go through some of the notable DNS hijackings throughout 2008 - [Comcast.net's DNS hijacking](#) ; [Photobucket.com's DNS hijacking](#) ; [ICANN and IANA's DNS hijacking](#))

Members of Team-Evil are no strangers to Israel. The group has been periodically [attacking pro-Israeli web sites since 2006](#) . Who are Team-Evil anyway?

Originally started as [a Moroccan-based hacking group](#) of Muslim hackers, today thanks to the group's popularity, they've managed to not only recruit more hackers/script kiddies, but also, gain the support of other Muslim hacking groups. The group's efficient way of exploiting Israeli and pro-Israeli web sites through commodity web site defacement tools scanning and exploiting known web application vulnerabilities reached such a peak, that a [17 years old member of Team-Evil got busted](#) . In the ongoing web site defacement attacks,

several other well known Muslim hacking groups appear to be working directly cooperating with **Team-Evil** , such as:

JURM-TEAM - members include sql_master, Jurm, Dr.Noursoft, RedDoom, Lpooxd, Cyb3rt and Dr.win

Islamic Cr3w - members include Twister and AIH7N00TY

TEAM SPECIAL AGENT - members include PrOf-HaCkEr,Black^Monster, FREEM@N, and R00t-Os

Team-Evil themselves - members include Jurm, Cyber-terrorist, J3ibi9a, Scritpx, Fatna Bant Hmida

It's important to point out that the massive web site defacements taking place are not rocket science, they are the low-hanging fruit made possible for them to abuse due to insecurely configured web servers. Interestingly, according to one of the messages left on the defaced sites, a separate campaign is launched by the Hamas supporters in response to [June, 2008's defacement done by Israeli hackers of the arabs48.com portal](#) .

(Go through related hacktivism attacks - [Hundreds of Dutch web sites hacked by Islamic hackers](#) ; [Pro-Serbian hacktivists attacking Albanian web sites](#) ; [300 Lithuanian sites hacked by Russian hackers](#))

Having monitored the demise of [international cyber jihadist hacking teams](#) (**Osama Bin Laden's Hacking Crew** , **Ansar AL-Jihad Hackers Team** , **HaCKErS aLAnSaR**) attacking primarily Western sites, in comparison Israel, Palestine and their supporters are not going to give up that easily the propaganda capabilities that [they've building since 2001](#) by means of web site defacements.

'This girl must be Out of her Mind to do this on live Television!' scam spreading on Facebook | ZDNet

Researchers from Sophos have intercepted a [currently spreading Facebook scam](#), enticing users into clicking on a bogus video link.

Spamvertised as:

Watch the embarrassing moment of her! It is really embarrassing.!

Upon clicking on the link users are tricked into sharing the link on their Facebook Walls by verifying their age. The scammers are monetizing the campaign using paid surveys as a means of monetization.

Users are advised to exercise extra caution when dealing with similar Facebook scams.

'The World Funniest Condom Commercial - LOL' scam spreading on Facebook | ZDNet

Security researchers from Sophos have spotted yet another scam currently spreading on Facebook. [The World Funniest Condom Commercial - LOL scam](#) attempts to trick users into clicking on the link which will eventually lead them to a bogus YouTube video screen.

Spamvertised as:

The World Funniest Condom Commercial - LOL haha its really so funny ~ Dont Miss it !

Upon clicking anywhere on the screen, users will then unknowingly "Like" the bogus video and further distribute it across Facebook. Users are advised to be extra vigilant when interacting with Facebook links, even those distributed by trusted friends, and take advantage of the [anti-clickjacking features](#) offered by the NoScript Firefox add-on.

The Web's most dangerous keywords to search for | ZDNet

Which is the most dangerous keyword to search for using public search engines these days? It's "*screensavers*" with a maximum risk of 59.1 percent, according to McAfee's recently released report "[The Web's Most Dangerous Search Terms](#)".

Upon searching for 2,658 unique popular keywords and phrases across 413,368 unique URLs, [McAfee's research](#) concludes that lyrics and anything that includes "free" has the highest risk percentage of exposing users to malware and fraudulent web sites. The research further states that the category with the safest risk profile are health-related search terms.

Here are more findings:

The categories with the worst maximum risk profile were lyrics keywords (26.3%) and phrases that include the word "free" (21.3%). If a consumer landed at the riskiest search page for a typical lyrics search, one of four results would be risky

The categories with the worst average risk profile were also lyrics sites (5.1%) and "free" sites (7.3%)

The categories with the safest risk profile were health-related search terms and searches concerning the recent economic crisis. The maximum risk on a single page of queries on the economy was 3.5% and only 0.5% risky across all results. Similarly, even the worst page for health queries had just 4.0% risky sites and just 0.4% risk overall

This isn't the first time McAfee is attempting to assess the risk percentage of particular search terms, as the company did similar studies in [2006](#) and [2007](#) . And whereas the research attempts to raise awareness on malicious practices applied by cybercriminals, it also has the potential to leave a lot of people with a false feeling of security since it's basically scratching the surface of a very dynamic problem.

With cybecriminals anticipating the dynamic nature of Web 2.0, they too, adapt dynamically to the changing environment. In the

context of blackhat SEO, like true marketers they apply basic mass marketing keyword practices, which may get wrongly interpreted as the use of particular keywords only.

In reality, mass marketing from blackhat SEO perspective means a very diverse set of topics usually consisting of hundreds of thousands of syndicated news/video/blog titles aggregated over a recent period of time, all operated by the same group. Therefore, the search term "screensavers" or any related phrases is among the hundreds of thousands of others part of a single malware campaign.

In October, 2008, cybercriminals taking advantage of blackhat SEO for malicious purposes, started [syndicating_popular_Google_Trends_keywords_in_real-time](#) in order to occupy the top ten search results with hundreds of automatically registered [Windows Live Spaces serving Zlob variants](#) as fake codecs back then. This dynamic approach not only undermines any static lists of "most dangerous keywords to search for", but also, tipped more cybercriminals on the basics of event-based blackhat SEO campaigns serving malware.

For instance, in an attempt to hijack the anticipated traffic of people searching for the [Twitter XSS worm StalkDaily/Mikeyy](#) , blackhat SEO campaigns using related keywords started appearing in public search engines serving scareware. At least that's what appeared at the first place, since a much more in-depth research revealed that the [Mikeyy keywords are part of a diverse blackhat SEO farm](#) . The same Ukrainian group took advantage of the swine flu buzz and launched another [blackhat SEO campaign](#) earlier this month, again consisting of swine flu related keywords in between the diverse set of topics that they've generated on the hundreds of domains participating.

Furthermore, taking into consideration the fact that nowadays legitimate and compromised web sites serve more exploits and malware than the purely malicious ones ([77% of Websites that carry malicious code are legitimate sites](#) ; [Thousands of legitimate sites SQL injected to serve IE exploit](#) ; [Over 1.5 million pages affected by the recent SQL injection attacks](#) ; [Gumblar - approximately 17,000 compromised sites](#)), a compromised web site's index would

undermine any such static lists of dangerous keywords to search for based on the diverse content that it's providing.

So, which is the most dangerous keyword to search for on the Web? That's a variable which cybercriminals play with at any moment.

The ultimate guide to scareware protection | ZDNet

Throughout the last two years, [scareware \(fake security software\)](#), quickly emerged as the single most profitable monetization strategy for cybercriminals to take advantage of. Due to the aggressive advertising practices applied by the cybercrime gangs, thousands of users fall victim to the scam on a daily basis, with the gangs themselves earning hundreds of thousands of dollars in the process.

Not surprisingly, [Q3 of 2009](#) was prone to mark the peak of the scareware business model, whose affiliate program revenue sharing scheme is not only attracting new cybercriminals due to its high pay-out rates, but also, is directly driving innovation within the cybercrime underground acting as a reliable financial incentive.

This end user-friendly guide aims to educate the Internet user on what scareware is, the risks posed by installing it, how it looks like, its delivery channels, and most importantly, how to recognize, avoid and report it to the security community taking into consideration the fact that 99% of the current releases rely on social engineering tactics.

What is scareware?

Basically, scareware, also known as rogueware or put in simple terms, fake security software, is a legitimately looking application that is delivered to the end user through illegal traffic acquisition tactics starting from **compromised web sites** ([Sony PlayStation's site SQL injected, redirecting to rogue security software](#)), **malvertising** ([MSN Norway serving Flash exploits through malvertising](#) ; [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Scareware pops-up at FoxNews](#) ; [Ukrainian "Fan Club" Features Malvertisement at NYTimes.com](#)), or **blackhat search engine optimization** ([9/11 related keywords hijacked to serve scareware](#) ; [The most dangerous celebrities to search for in 2009](#) ; [The Web's most dangerous keywords to search for](#)), to ultimately attempt to trick the user into believing their computer is already infected with

malware, and that purchasing the application will help them get rid of it.

Upon execution, certain scareware releases will not only prevent legitimate security software from loading, but it will also prevent it from reaching its update locations in an attempt to ensure that the end user will not be able to get the latest signatures database. Moreover, it will also attempt to make its removal a time-consuming process by blocking system tools and third-party applications from executing.

There have also been cases where scareware with elements of [ransomware](#) has been encrypting an infected user's files, [demanding a purchase in order to decrypt them](#) , as well as a single reported incident where a [scareware domains was also embedded with client-side exploits](#) .

For the time being, scareware releases are **exclusively targeting Microsoft Windows users** .

The characteristics of scareware - pattern recognition for a scam

Due to the fact that the scareware campaigns maintained by partners in the affiliate network use a standard template distributed to all of them, scareware sites all share a very common set of deceptive advertising practices, which can easily help you spot them before making a purchase.

For instance, the majority of scareware sites attempt to build more authenticity into their propositions by using **"non-clickable" icons of reputable technology web sites** and performance evaluating services, such as *PC Magazine Editors' Choice award* , *Microsoft Certified Partner* , *ICSA Labs Certified* , *Westcoast Labs Certified* , *Certified by Softpedia* , *CNET Editors' Choice* , as well as [ZDNet Reviews](#) -- the real [ZDNet Reviews](#) are unaware of the scareware's existence.

[Next](#) -->

Yet another popular social engineering tactic are the **fake comparative review templates** , basically showing a chart where

the scareware outperforms software offered by some of the leading security companies.

Since the end user who's about to conduct an impulsive purchasing decision, doesn't have the time to double check these claims, the attached screenshot indicates how three different scareware brands (*Virus Shield 2009* , *Windows Security Suite* and *Malware Destructor 2009*) are all using the same template claiming their superiority over legitimate security software.

The diverse list of tactics leads us to the ubiquitous fear-driven social engineering tactic of **simulating a real-time antivirus scanning in progress dialog** , which in reality is nothing else but a static script, with anecdotal cases where Mac users are presented with a Windows-like My Documents folder window.

The scanner's results are static, fake and have absolutely no access to your hard drive, therefore the claims that "*You're Infected!; Windows has been infected; Warning: Malware Infections found; Malware threat detected* " should be considered as a **fear mongering tactic** .

Legitimate online malware scanners offered for free by their vendors include, but are not limited to:

[TrendMicro's Housecall](#) [Kaspersky's Online Malware Scanner](#) [E-Secure's Online Malware Scanner](#) [ESET's Online Malware Scanner](#) [BitDefender's Online Malware Scanner](#) [PandaSecurity's Cloud Antivirus](#) [McAfee's Online Malware Scanner](#) [Rising's Online Malware Scanner](#) [Dr. Web's Online Malware Scanner](#) [Symantec's Online Malware Scanner](#) [CA's Online Malware Scanner](#)

Among the key characteristics of scareware remain the professional site layout, as well as the persistent re-branding of the template in an attempt to shift the end user's attention from the previous brand's increasingly bad reputation across the web. Combined, these characteristics result in an efficient social engineering driven scam that continues tricking thousands of victims on a daily basis.

[Next](#) -->

The delivery channels and traffic hijacking tactics of scareware campaigns

There's a high probability that your last encounter with scareware came totally out of blue. Despite the fact that cybecriminals are always looking for new push and pull strategies for their malware releases, there are several tactics currently representing the most popular delivery channels for scareware. Let's review some of them.

Blackhat search engine optimization (SEO) - blackhat search engine optimization remains [the traffic acquisition method of choice for the majority of cybercriminals](#) looks for quick ways to hijacking as much traffic as possible using real-time events as themes for their campaigns. This tactic consists of hundreds of thousands of hijacked keywords parked on domains maintained by the criminals. Upon visiting any them, the now tricked into believing the site is serving legitimate content end user, is automatically redirected to a simulated real-time antivirus scanning screen.

The [relevance of the themes](#) is automatically [syndicated from public services](#) such as [Google Trends](#) in order to ensure that the window of opportunity for a [particular event is hijacked for the purpose of serving scareware](#) . It's important to point out that each and every campaign relies on the end user's gullibility into manually downloading and executing the scareware compared to drive-by attacks where the infection will take place automatically through the use of client-side vulnerabilities.

Some of most recent and still ongoing blackhat SEO campaigns include - [9/11 related keywords hijacked to serve scareware](#) ; [Federal forms themed blackhat SEO campaign serving scareware](#) and [News Items Themed Blackhat SEO Campaign Still Active](#)

Systematic abuse of social networks/Web 2.0 services - there hasn't been a single social network or Web 2.0 service that hasn't been abused for scareware serving purposes. From [Twitter](#) , [Scribd](#) and [LinkedIn](#) to [Digg](#) and [Google Video](#) , the systematic abuse of these services through the automatic registration of hundreds of accounts by [outsourcing the CAPTCHA-recognition process](#) , remains an active asset in the arsenal of the scareware campaigner **Malvertising** (malicious advertising) - [malvertising](#) is the practice of

serving malicious ads on legitimate and high profile sites in an attempt to exploit the end user's trust in their ability to filter out such ads. Notable cases where scareware windows pop-up out of the blue include - [Fake Antivirus XP pops-up at Cleveland.com](#) ; [Scareware pops-up at FoxNews](#) , [Digg, MSNBC and Newsweek scareware campaign through malvertising](#) **Pushed by some of the most prolific botnets such as Conficker and Koobface** - The [Koobface botnet gang](#) which I've been tracking over the [past couple of months](#) , is not only among the most active [blackhat SEO cybercrime enterprises](#) online -- at least for the time being -- but there have been cases where they've been directly installing [scareware on Koobface infected hosts](#) . Despite its current idleness, the Conficker botnet gang has already made three attempts to monetize the millions of infected hosts, by [reselling access to them](#) to two [different gangs](#) , but has also [attempted to install scareware](#) on them

Now that you know what scareware is and how it reaches you, it's time to review some of practical ways for recognizing, avoiding and reporting it to the security community for further analysis.

[Next](#) -->

Recognizing, avoiding and reporting scareware

Recognizing the bad apples and flagging them

Due to the dynamic and constant re-branding of known scareware releases, maintaining a list of brands to recognize, avoid and be suspicious about is highly impractical.

However, the most logical approach in that case would be to **maintain a list of legitimate antivirus software vendors** in an attempt to raise more suspicion on those who are not within the list. [One such list is maintained by the CCSS](#) (Common Computing Security Standards Forum), and for the time being includes the following vendors:

AhnLab (V3) Antiy Labs (Antiy-AVL) Aladdin (eSafe) ALWIL (Avast! Antivirus) Authentium (Command Antivirus) AVG Technologies (AVG) Avira (AntiVir) Cat Computer Services (Quick Heal) ClamAV (ClamAV) Comodo (Comodo) CA Inc. (Vet) Doctor Web, Ltd. (DrWeb) Emsi Software GmbH (a-squared) Eset Software

(ESET NOD32) Fortinet (Fortinet) FRISK Software (F-Prot) F-Secure (F-Secure) G DATA Software (GData) Hacksoft (The Hacker) Hauri (ViRobot) Ikarus Software (Ikarus) INCA Internet (nProtect) K7 Computing (K7AntiVirus) Kaspersky Lab (AVP) McAfee (VirusScan) Microsoft (Malware Protection) Norman (Norman Antivirus) Panda Security (Panda Platinum) PC Tools (PCTools) Prevx (Prevx1) Rising Antivirus (Rising) Secure Computing (SecureWeb) BitDefender GmbH (BitDefender) Sophos (SAV) Sunbelt Software (Antivirus) Symantec (Norton Antivirus) VirusBlokAda (VBA32) Trend Micro (TrendMicro) VirusBuster (VirusBuster)

An alternative list of [legitimate antivirus software providers](#) is also maintained by the VirusTotal service.

If you're serious about security and care about your data, you wouldn't trust your computer's integrity to an application called *Doctor Antivirus 2008* , *Spyware Preventer 2009* , *Power Antivirus* , *Total Virus Protection* , *Malware Destructor 2009* , *Cleaner 2009* , *Smart Antivirus 2009* , *Antivirus VIP* or *Advanced Antivirus 2009* , would you?

Another practical step in recognizing scareware, is to **research the potentially malicious domain** in question by either using Google.com, or an [investigative search engine](#) maintained by Google's Anti-Malvertising.com project. The search engine is using a database of sites maintaining lists of scareware related domains, and greatly increases the probability of seeing the suspicious domain in the results.

Keeping in mind that the end user has full control of the scareware window that popped-up on their screen -- despite its modest resistance when attempting to close it down -- downloading a copy of it, and once making sure you're not going to execute it, **submit it to a multiple antivirus scanning service** such as [VirusTotal.com](#) to further ensure its real nature, may in fact help protect millions of users across the globe against this particular release since the service shares the malware binaries across multiple vendors.

The file submitted on the attached screenshot may not be detected by your antivirus vendor as scareware, but has already been flagged as scareware by several other.

Avoiding and preventing the scareware campaign

As in real-life virus outbreak, **prevention is always better than the cure** . In terms of scareware, handy Firefox-friendly [add-ons such as NoScript](#) -- which you can see in action against an ongoing scareware campaign -- can undermine the effectiveness of any scareware campaign, delivered through any of the distribution channels already discussed.

In a fraudulent scheme relying exclusively on social engineering tactics, fear in particular, and a business model that's largely driven by the end user's lack of awareness on this nearly perfect social engineering scam, vigilance, absence of gullibility and common sense suspicion remain your best protection.

Consider going through the "[The ultimate guide to scareware protection](#)" gallery

Have you been a victim of scareware, or has a scareware brand ever popped-up on your screen while browsing a legitimate web site? What do you think is the main reason why thousands of users purchase fake security software on a daily basis? Their lack of awareness on the fraud scheme, or gullibility by default?

Talkback .

The Storm Worm would love to infect you | ZDNet

The Storm Worm malware is back in the game, with its most recent campaign currently active and trying to entice users into executing **iloveyou.exe** by spamming them with links to already infected hosts acting as web servers, next to SQL injecting malicious domains into legitimate sites for the campaign to scale faster.

What has changed compared to previous campaigns? Storm Worm is back in the SQL injection attack phrase, with **tellicolakerealty .cn/ind.php** iframe injected at a small of sites for the time being. Moreover, assessing the storm worm infected hosts can only be done if you spoof your user agent to Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1921), otherwise you will get no indication for any kind of malicious activity going on. Furthermore, despite that there are no exploits used at the infected hosts but, a heavily obfuscated **HTML/Rce.Gen** was detected in their injected domain which would load automatically upon someone visiting an already injected site.

These are the most recent detection rates for both, the binary, and the javascript obfuscation :

Javascript obfuscation Scanners result : 6/32 (18.75%)
HTML/Rce.Gen; Packed.JS.Agent.a

iloveyou.exe Scanners result : 10/32 (31.25%) **Email-Worm.Win32.Zhelatin.yu; Trojan.Peed.PJ**

Compared to the previous event-based social engineering campaigns on behalf of Storm Worm, the latest wave of malware isn't thematic at all. It remains to be seen whether or not they would start emphasizing on SQL injections to acquire new infected hosts given the success of the copycats and [the Asprox botnet](#) , or continue using email as the primary distribution vector.

The security and privacy ramifications of AT&T's iLeak | ZDNet

A French group of security researchers, has obtained [the emails of 114,000 iPad users](#) who signed up for AT&T's 3G wireless service, including their associated [ICC-IDs](#), relying on a flaw in the company's site which allowed them to automate the process.

Does this leak pose any security, privacy, or perhaps even national security risks due to the leaked U.S Department of Defense, U.S Army and DARPA emails? **Update:** [FBI launches probe over AT&T's iPad breach](#)

UPDATED: Tuesday, June 15, 2010: Due to the anticipated ["What If"](#) scenarios, and many direct questions that I'm receiving, the following update including comments from Goatse Security and Gawker, aims to clarify the situation.

[Chris Paget comments on the incident:](#)

"I'm somewhat of an authority on GSM security, having given presentations on it at [Shmoocon](#) (M4V) and [CCC](#) (I'm also scheduled to talk about GSM at this year's Defcon). This is my take on the [iPad ICCID disclosure](#) — the short version is that (thanks to a bad decision by the US cell companies, not just AT&T) ICCIDs can be trivially converted to [IMSI](#) s, and [the disclosure of IMSIs leads to some very severe consequences](#) , such as name and phone number disclosure, global tower-level tracking, and making live interception a whole lot easier. My recommendation? AT&T has 114,000 SIM cards to replace and some nasty architectural problems to fix."

According to the [statement issued by the group](#), they have not **just erased the emails+ICCIDs** , but **haven't shared them with anyone else but Gawker** . Moreover, given the fact that **there's no known public copy of the emails+ICCDs** (as of June 15th, 2010), for researchers to experiment with, **you can always request a new SIM card from AT&T** , if you're uncomfortable with the incident that took place.

Asked to comment on the case, both, Goatse Security (Escher Auernheimer) and Gawker (Remy Stern) had the following to say.

Q: Once the harvested emails were obtained, were they shared with anyone else, but Gawker's reporter, or posted online in any form?

Goatse Security: No, they were only shared with Gawker who agreed to responsibly redact them to not reveal any personally identifying information. We did not post them online nor publish them as many have alleged. We destroyed the data after we gave it to Gawker, to prevent loss and security risks.

Q: Are you aware of whether Gawker's reporter did the same, namely erase the content, and not share the data with anyone else?

Goatse Security: I do not know if Ryan Tate destroyed his copy of the data. I believe he has been ordered by the FBI to retain it, so any potential breach of the data's security there would be the responsibility of the federal government.

Q: Did you share a copy of the PHP script with anyone? And if yes, was a copy of the script shared BEFORE the flaw was fixed, or AFTER it was fixed making the script virtually useless?

Goatse Security: A version of the script was potentially stored in an insecure fashion when the original author first made it. At this point in time we were lacking an additional bit of data that did not allow us to understand the full ramifications of the vulnerability. We have no evidence that it was retrieved or used by anyone else and made a best effort to lock it down and publicly disclose the vulnerability as soon as we had an understanding of the scale of AT&T's data exposure. As everyone at GS had other priorities when the script was first written it was not until later until it was tested and made a high priority on our groupware. Unfortunately for the consumer, our commercial priorities have to take precedence over our charitable public interest ones.

Q: Since Goatse claims to have erased the data, and have never shared it with anyone else but with Gawker, did you do the same, namely, not share it with anyone else, and delete it?

Gawker: No, we did not share the data with anyone else nor do we have any plans to do so. The printed copy of the data, which was depicted in our original story, was shredded immediately after the photograph was taken.

We do continue to possess a digital copy of the file. Per the preservation notice we received from last week from federal authorities, we have retained all our files related to the story, as was requested of us.

The security risks posed by this email leak, are pretty similar to the security risks from related compromises, with the potential malicious attackers now sitting on hundreds of thousands of email accounts. Here are two of the most common abuse scenarios that could take place:

Targeted malware/phishing attacks impersonating Apple Inc.

- [Spear phishing attacks](#) are emails specifically crafted for a particular targeted group, attempting to capitalize on a particular event. In this case, potential attackers could easily execute such an attack impersonating Apple's response to the situation/mitigation practices, knowing that the owners of these emails are now particularly susceptible to interacting with such emails.

Targeted malware/phishing attacks impersonating AT&T - This scenario is identical to first one, however, this time it's AT&T's response/mitigation practices that could be used as social engineering lure. And although I don't really think there's going to be a significant outbreak of such campaigns, due to the fact that the rest of their campaigns are producing the results they desire, the possibility for abuse remains.

The following is brief FAQ summarizing the most important aspects of AT&T's iLeak incident:

How did Goatse Security manage to obtain the emails and associated ICC-IDs? - The group ([listen to a podcast with one of the researchers](#)) appears to have automated the brute forcing process using a script with which they fed the AT&T's site with spoofed user-agents (iPad) and random ICC-IDs numbers, in between recording all the valid emails that were returned for a correct ICC-ID. The last time, a similar attempt abusing weak

security practices was seen in the wild, resulted in thousands of leaked confidential/nude photos of the [photo sharing iPhone app Quip](#).

What are the privacy ramifications of the leak, if any? - Despite the leaked emails of top executives at the New York Times Company, Dow Jones, Condé Nast, Viacom, Time Warner, News Corporation, HBO, Goldman Sachs, JP Morgan, Citigroup, Morgan Stanley etc. the only case where the incident would pose a privacy risk to these executives, is when these email accounts weren't published on the Web in the first place. Moreover, despite [claims that average users can obtain the physical location of an iPad's user through the leaked ICC-ID](#), that's not really the case. The [physical location is already known to the mobile carrier](#) using plain simple triangulation and related techniques used by law enforcement agencies, with or without the possession of the ICC-ID.

Does the leak pose any national security risks due to the sensitive nature of the emails involved? - Depends on the perspective and degree of paranoia, although the U.S Intelligence Community is definitely not happy with the fact that a particular U.S Department of Defense, U.S Army or DARPA email can now be associated with a [ICC-ID](#) that leaked on the Web. Meanwhile, the [NYTimes has already responded by asking iPad users to turn off access to the 3G network](#) - *"As our security team and network engineers investigate the full extent of the breach via Apple and AT&T, we suggest that you turn off your access to the 3G network on your iPad until further notice. "*

Did AT&T issue a response to the incident? - The following is the company's official response to the situation: *AT&T was informed by a business customer on Monday of the potential exposure of their iPad ICC IDs [used to authenticate the subscriber on AT&T's network]. The only information that can be derived from the ICC IDs is the e-mail address attached to that device. This issue was escalated to the highest levels of the company and was corrected by Tuesday; and we have essentially turned off the feature that provided the e-mail addresses. The person or group who discovered this gap did not contact AT&T. We are continuing to investigate and will inform all customers whose e-mail addresses and ICC IDs may have been*

obtained. At this point, there is no evidence that any other customer information was shared. We take customer privacy very seriously and while we have fixed this problem, we apologize to our customers who were impacted.

Although the iLeak is an embarrassing moment for both, AT&T and Apple, the incident only adds a small additional risk to the ones users are currently facing, such as [malware, phishing, blackhat SEO, and client-side exploitation](#) through unpatched 3rd party applications.

What it proves through, is what independent data breach reports have been saying for years - [in the majority of cases a third-party business partner was usually responsible for the breach](#).

Are you affected by this incident, and somehow concerned about your privacy. What's your main concern? Do you believe that the leak of unpublished emails belonging to company executives, would somehow affect them? How about the ones belonging to the DOD, DOJ and DARPA? Who's to blame for this incident, Apple for trusting AT&T's ability to securely operate with the data, or AT&T for allowing this to happen?

TalkBack.

The Pirate Bay hacked through multiple SQL injections | ZDNet

According to an advisory posted on the web site of Argentinian group of security researchers, they were able to [obtain access to the Pirate Bay's administration panel](#), by discovering multiple SQL injections, leading to the exposure of emails, MD5 hashes for passwords, and the IP address for any particular Pirate Bay user.

The video produced by the group, shows the user names of uploaders, associated emails and IP addresses, reasons for getting banned, including detailed logs of their activities on the tracker. Strangely enough, the Pirate Bay appears to have a special "*List 100 newest users with GMail* " feature, next to the searchable database of emails.

A similar [hacking incident affected the tracker](#) in 2007.

The web site of the Pirate Bay is currently returning the following message "*Upgrading some stuff, database is in use for backups, soon back again.. Btw, it's nice weather outside I think.* " indicating that they're aware of the compromise.

The Neosploit cybercrime group abandons its web malware exploitation kit | ZDNet

[The end of the Neosploit](#) web malware exploitation kit? [RSA's FraudAction Research Labs](#) recent monitoring of ongoing

communications between Neosploit team members and their potential customers indicates so. The Neosploit malware kit has been around since the middle of 2007, with prices varying between \$1000 and \$3000, whose main differentiation factors next to its popular alternatives such as MPack and Icepack, were its customer support and the constant updates, including new javascript obfuscation routines and exploits as they were made available, its multi-user command and control interface, as well as the improved metrics and filtering of infected hosts.

Is this really the end of Neosploit? Could be, but it's definitely not the end of web malware exploitation kits in general :

"In mid-July, however, evidence showed that Neosploit's successful business was running into problems. It is likely that Neosploit was finding it difficult to sustain its new customer acquisition rate, and that its existing customers were not generating enough revenue to sustain the prior rate of development. These problems appear to have been too much of a burden, and we now believe that the Neosploit development team has been forced to abandon its product. Like any responsible business, the Neosploit team is trying to be remembered as a good business that might one day return. Our sources reported that they took the time and effort to part properly with an "out of business" announcement. Or as the translation goes:

"Unfortunately, supporting our product is no longer possible. We apologize for any inconvenience, but business is business since the amount of time spent on this project does not justify itself. We tried hard to satisfy our clients' needs during the last few months, but the support had to end at some point. We were 1.5 years with you and hope that this was a good time for your business."

Let's discuss their business model, how other cybercriminals disintermediated it thereby ruining it, and most importantly, how is it possible that such a popular web malware exploitation kit cannot seem to achieve a positive return on investment (ROI).

The short answer is - piracy in the IT underground, and their over-optimistic assumption that high-profit margins can

compensate the lack of long-term growth strategy, which in respect to web malware exploitation kits has do with the benefits coming from converging with traffic management tools. Let's discuss some key points.

You cannot pitch an open source malware kit as a proprietary one

Neosploit, just like the majority of other web malware kits, are open source, which means the customer can add new functions and exploits, enjoying the malware kit's modularity. Neosploit Team's business model was relying on the wrong assumption that charging thousands of dollars for a proprietary malware kit with the idea to position it as exclusive one could result in a high-growth business model. Moreover, according to their statement that the amount of time spend on the "product" isn't justifying itself wrongly implies that it takes a great deal of time to embedd a publicly available exploit code for a recent vulnerability into the while, while in reality it doesn't.

Furthermore, the coders of [crimeware kits like Zeus for instance](#) , have tried to enforce "licensing agreements", ironically by doing so they [claim ownership over the crimeware kit in general](#) . In fact, coders of malware for hire are taking advantage of the same end user agreements, forbidding the customer of [reverse engineering the malware they've just coded](#) , and also sharing it with others. And so, the Neosploit kit leaked into the wild, for script kiddies and sophisticated attackers to take advantage of, from here no one was bothering to purchase a copy of the malware kit, and started persinally embedding new exploits within.

Localization to foreign languages is done on behalf of the customers, not the malware kit's coders

One would logically assume that if a Russian malware coder wants to target potential customers from China, he'd bother translating the entire command and control interface next to the documentation of the malware kit into the local language. In reality through, [this localization has been done mainly on behalf of users](#) who've obtained leaked copies of the malware kits and localized them into their native languages, thereby allowing easier entry into cybercrime in general. For instance, the originally Russian [MPack and IcePack malware kits were localized to Chinese](#) by Chinese hackers last year, the same [localization of the Firepack malware kit to Chinese](#) took place this May, and surprisingly, [IcePack got localized to French](#) the same month.

Web malware exploitation kits are a commodity

Namely, they are easy to obtain, and even easier to use even by those who're not familiar with Russian. This commoditization directly ruined the business model, and among the main reasons why the Neosploit Team is stopping the support of their malware kit, is mainly because they're no longer feeling comfortable being used as the foundation for someone else's successful malware attack. However, the open source nature of the malware kits is directly resulting in an unknown number of modified malware kits using the publicly ones as a foundation to build and add new features on. This fact makes it a bit irrelevant to count and keep track of which and how many exploits are included within a particular kit, since the number will only be valid for this particular copy of the kit.

The again, when you have [637 million Google users surfing with insecure browser](#) and getting exploited with "last quarter's critical browser vulnerability", why bother introducing zero day vulnerabilities within your kit when outdated and already patched ones seems to achieve such a high success rate of infection anyway?

Today's international script kiddies are empowered with localized versions of sophisticated web malware exploitation kits courtesy of Russian hackers, seems like globalization in action. The Neosploit Team may be abandoning support for their malware kit, but they're

so not abandoning the current malware campaigns they manage using it.

The most dangerous celebrities to search for in 2009 | ZDNet

Searching for which celebrity has the highest probability of tricking you into visiting a malware-friendly web site?

[Last year it was Brad Pitt](#) , but according to this year's McAfee report "[Riskiest Celebrities to Search on the Web](#) ", it's Jessica Biel related searches that have *"one in five chance of landing at a Web site that's tested positive for online threats, such as spyware, adware, spam, phishing, viruses and other malware "*.

Just like previous editions of the report, the latest one has also excluded the dominant [adult content theme](#) , as well as the fact that static lists of dangerous keywords to search for are long gone from the arsenal of the experienced blackhat SEO campaigner. In 2009, cybercriminals enjoy the benefits of the real-time Web at its best, by dynamically serving malware based on trending topics, or occupying as many keywords as possible through [blackhat SEO \(search engine optimization\) tactics](#) .

A good example of the current situation is an ongoing malicious campaign abusing Digg's high page rank, which is redirecting to scareware-serving sites by hijacking keywords related to any of the [top 15 celebrities listed in McAfee's report](#) .

Go through related posts: [The Web's most dangerous keywords to search for](#) ; [Cybercriminals hijack Twitter trending topics to serve malware](#) ; [Cybercriminals syndicating Google Trends keywords to serve malware](#) ; [Federal forms themed blackhat SEO campaign serving scareware](#) ; [Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign](#) ; [Google Video search results poisoned to serve malware](#) ; [Massive comment spam attack on Digg.com leads to malware](#)

Taking into consideration Digg's high page rank and the near real-time crawling of Digg submitted content, cybercriminals are systematically abusing major Web 2.0 services in order increase the visibility of their malicious content. Moreover, not only are they

diversifying the themes, but also, by abusing multiple Web 2.0 services there are instances where the first 10 search results for a particular keyword are all populated by malicious sites part of a single campaign.

The bottom line is that any celebrity related search can lead to a malicious site depending on the momentum of a particular campaign, or the type of theme the cybercriminal chose to use. Therefore, relying on static lists for potentially dangerous keywords is unrealistic in a cybercrime ecosystem that's taking advantage of the traffic peak momentum in real-time.

The most "dangerous" celebrities to search for in 2008 | ZDNet

Searching for details regarding the latest celebrity gossip may expose you to everything the IT underground has to offer - from adware and spyware to misleading offers and fake newsletters enticing you to opt-in into a spammer's campaign. McAfee owned SiteAdvisor has recently released [the 2008 list of the celebrity names that are most actively abused by malicious attackers](#) in order to attract legitimate traffic to their malicious sites.

01. Brad Pitt -- When "Brad Pitt screensavers" was searched, more than half of the resulting Web sites were identified as containing malicious downloads with spyware, adware and potential viruses.

02. Beyonce -- Inputting "Beyonce ringtones" into a search engine yields risky Web sites that promote misleading offers to gather consumers' personal information.

03. Justin Timberlake -- Interest in his high-profile relationships makes him an easy target for spammers and hackers. When searching for "Justin Timberlake downloads" one Web site advertised free music downloads that were flagged as directly leading to spam, spyware and adware.

04. Heidi Montag -- "The Hills" star is a popular search term when it comes to searching for wallpaper. A host of wallpaper Web sites contained hundreds of malware-laden downloads.

05. Mariah Carey -- Spammers and hackers are using Mariah Carey screen saver Web sites to link to other sites proven to contain spyware, adware and other threatening downloads."

Who else is on the list?

Celebrities like the following in order of maliciousness - Jessica Alba, Lindsay Lohan, Cameron Diaz, George Clooney, Rihanna, Angelina Jolie, Fergie, David Beckham, Katie Holmes, Katherine Heigl.

With the research originally based on SiteAdvisor's rankings for related celebrity sites, it's basically scratching the surface

since these sites are only the tip of the iceberg beneath which lies an extensive network of blackhat search engine optimization campaigns and [comprehensive portfolios](#) of domains serving [fake celebrity sites](#) pushed in the form of spam. This approach is not exclusively targeting a particular celebrity more than another, it's targeting all of them. Moreover, searching means that the end user is "pulling" the malicious sites, whereas "pushing" them through spam, blackhat SEO seems and SQL injections in order to acquire traffic, remains the tactic of choice. These traffic acquisition tactics are also abusing legitimate services like Blogspot, Google Groups or MSN Groups, instead of using separate domains and are consequently not flagged as malicious but reputation based services like SiteAdvisor.

With multiple vendors and security researchers continuing to see evidence that legitimate sites have started serving more malicious content than on purposely registered malicious domains, you may in fact be more susceptible to an attack while browsing your favorite site, than searching for a particular celebrity. And even if you don't search for the celebrities, the celebrities are always searching for you, just check your spam/malware folder.

The most common iPhone passcodes | ZDNet

Wonder which is the most popular lockscreen PIN?

Daniel Amitay, the developer of the Big Brother Camera Security iPhone app has been [collecting aggregate data on the use of lockscreen PINs](#) of users of his application. Based on a sample of 204,000 passcodes, here are the most popular passcode choices:

1234
0000
2580
1111
5555
5683
0852
2222
1212
1998

Not surprisingly, the ubiquitous 1234 occupies the top position. The research data further examines the connection between the passcode choice and the different numbers, and find out that "with a 15% success rate, about 1 in 7 iPhones would easily unlock--even more if the intruder knows the users' years of birth, relationship status, etc"

Related posts: [Researchers use smudge attack, identify Android passcodes 68 percent of the time](#); [And the most popular password is...](#)

The research data excludes [password re-use patterns](#), therefore it's fairly logical to assume that the same insecure passcode choosing patterns can be seen elsewhere as well.

The Kneber botnet - FAQ | ZDNet

A recently uncovered [network of compromised hosts](#) dubbed, the "[Kneber botnet](#)", managed to successfully infect 75,000 hosts within over 2,500 organizations internationally, including Fortune 500 companies as well as Local, State and U.S Federal Government agencies.

How did the botnet managed to stay beneath the radar? Who's behind it? Is it an isolated underground project, or a part of the malicious portfolio of a cybercrime organization diversifying on multiple fronts within the underground marketplace?

Go through the FAQ.

01. Why the name Kneber botnet?

The name Kneber comes from the email used to register the initial domain, used in the campaign - **HilaryKneber@yahoo.com** . What's particularly interesting about this email, is the fact that it was also profiled in December, 2009's "[Celebrity-Themed Scareware Campaign Abusing DocStoc](#)" analysis, linking it to money-mule recruitment campaigns back then.

02. My time is precious. In short, what is the Kneber botnet at the bottom line?

It's a mini [Zeus crimeware botnet](#) , one of the most prevalent malicious software that successfully undermining two-factor authentication on the infected hosts ([Report: 48% of 22 million scanned computers infected with malware](#)), and is slipping through signatures-based antivirus detection ([Modern banker malware undermines two-factor authentication](#)) due to the systematically updated binaries.

03. Who's behind it?

It's a cybercrime syndicate involved in everything from blackhat search engine optimization (blackhat SEO), to client-side exploit serving campaigns, and money mule recruitment campaigns.

04. What were the botnet masters able to steal from the infected hosts?

Surprisingly, in the sense that the Zeus crimeware is exclusively used to steal financial data, and hijack E-banking transactions on-the-fly, in the case of the Kneber botnet, researchers from NetWitness found just 1972 digital certificates, and over 68,000 stolen credentials over a period of 4 days.

05. Is this botnet part of a sophisticated cybercrime enterprise vertically integrating by engaging in multiple fraudulent activities, or is it an isolated underground project?

The Kneber botnet is anything but an isolated project, with the individual/group of individuals managing it already connected to numerous malicious campaigns analyzed over the last couple of months. Here are some interesting facts about their activities:

The name servers used in [December, 2009's DocStoc scareware campaign](#) , were registered using the same email used to register the [client-side exploit serving domains](#) part of the Koobface gang's experiment conducted in November, 2009. Parked on the same IP hosting the domain which was serving the malware in the campaign, was also the a domain registered to **HilaryKneber@yahoo.com** (search-results .cn) Even more interesting is the fact that the emails used to registered the rest of the domains parked at this IP, are also known to have been used in registering money mule recruitment domains ([Standardizing the Money Mule Recruitment Process](#) ; [Keeping Money Mule Recruiters on a Short Leash](#)) [According to the report](#) , the email **HilaryKneber@yahoo.com** itself was also used to registered a [money mule recruitment company known as 24 Hour Express Service](#) The report further establishes a connection between the Waledac botnet and this mini Zeus botnet, with the two malware families found simultaneously on the same hosts. An excerpt from the report: *"One very interesting observation is that more than half of the ZeuS bots are logging traffic from additional infections on the same host that are indicative of Waledac command and control traffic. Waledac is a peer-to-peer spamming botnet that is often used as a delivery mechanism for additional malware. Additional analysis needs to be conducted, but this raises*

the possibility of direct enterprise-to-enterprise communication of Waledac bot peers in addition the existing C2 traffic from the Zeus botnet. "

This isn't the first time Waledac connection is established between different botnets - "[Waledac is Storm is Waledac? Peer-to-Peer over HTTP.. HTTP2p?](#) "; "[Walking Waledac](#) "; "[..Conficker downloading the Waledac e-mail worm onto the infected systems](#) "; "[..Downad/Conficker box was trying to access a known Waledac domain](#) "

06. What's so special about it?

It's the fact that despite the crimeware's advanced E-banking sessions hijacking, the primary objective of their campaign -- at least based on the sample analyzed by NetWitness researchers -- was to steal social networking credentials.

Moreover, the Kneber botnet is a good example of an ongoing trend aiming to build and maintain beneath the radar botnets ([Research: Small DIY botnets prevalent in enterprise networks](#) ; [Inside the botnets that never make the news - A Gallery](#) ; [Aggregate-and-forget botnets for DDoS extortion attacks](#))

And while NetWitness is logically not offering insight into which companies were most affected, but the usual vertical market data, based on 74,000 infected PCs at nearly 2,500 organization, we can assume a proportional scenario with 29.6 infected hosts per company, representing your typical small DIY botnet.

07. What's the OS breakdown of the infected hosts?

The top five affected operating system versions based on the [data presented by NetWitness](#) are: *XP Professional SP 2* , followed by *XP Professional SP 3* , *XP Home Edition SP 3* , *XP Home Edition SP2* and *Vista Home Edition SP 2* .

When discussing botnets in general, it's important to keep in mind that botnets aggregated by using the Zeus crimeware, are not the same type of botnets like Conficker, Pushdo or Koobface which rely exclusively on "proprietary malware code". In compassion, due to the fact that Zeus is a DIY (do-it-yourself) type of crimeware, it allows

potential cybercriminals to literally generate crimeware variants on their own.

The future of mobile malware - digitally signed by Symbian? | ZDNet

Earlier this month, a mobile malware known as [Transmitter.C](#), [Sexy_View](#), [Sexy_Space](#) or [SYMBOS_YXES.B](#), slipped through [Symbian's mobile code signing procedure](#), allowing it to act as a legitimate application with [access to device critical functions](#) such as access to the mobile network, and numerous other functions of the handset.

Upon notification, [the Symbian Foundation quickly revoked the certificate](#) used by the bogus Chinese company [XinZhongLi TianJin Co. Ltd](#), however, due to the fact the revocation check is turned off by default, the effect of the revocation remains questionable.

What are the chances that future malware authors could [bypass the code signing procedure](#) again?

Before answering the question, it's worth pointing out how they manage to do it in the first place. [According to F-Secure](#), the authors of [SYMBOS_YXES.B](#) seem to have digitally signed their malware by using the Express Signing procedure, taking advantage of the lack of human inspection. Another variant of the [malware was also digitally signed](#) in February.

The [missing human inspection](#), instead of the total reliance on mobile antivirus scanner, could have prevented the signing of the malware, since the malware authors didn't even bother to create a fake company page on the Internet in an attempt to improve their legitimacy. For instance, none of the previously used Chinese company names (**XiaMen Jinlonghuatian Technology Co. Ltd.**, **ShenZhen ChenGuangWuXian Tech. Co. Ltd.** and **XinZhongLi TianJin Co. Ltd.**) have any public reference.

And while the mobile malware campaign is not necessarily widespread, it remains active, with the malware domain SMS-ed still online, and hosted by the U.S based Global Net Access (GNAX), which hasn't responded to abuse notifications throughout the past 30 days.

The Symbian Foundation is investigating how they can improve the signing procedure, and detect malware before they issue yet another certificate to its authors. Over [2000 applications go through the signing process](#) each month.

The EFF releases new HTTPS Everywhere Firefox extension | ZDNet

The Electronic Frontier Foundation, in a cooperation with the Tor Project, [has released a beta version](#) of the "[HTTPS Everywhere](#) " Firefox extension.

The extension helps users encrypt their traffic to a small, but growing number of high profile sites, by forcing full-session HTTPS connections.

According to the EFF's announcement, the extension currently works on the following sites:

Google Search, Wikipedia, Twitter, Facebook, The New York Times, The Washington Post, Paypal, EFF, Tor, Ixquick

Does "HTTPS Everywhere" really mean "Privacy Everywhere"? Not necessarily, and here's why it may leave a lot of users with a false feeling of privacy:

Full-session HTTPS may prevent interception of some of your activities -- unless of course [there's a weak link](#) somewhere -- however, it doesn't hide your IP, doesn't use any sort of [mixing tactics](#) , potentially allowing the leak of personally identifiable information to Google, and [doesn't prevent](#) alternative [tracking activities](#) from taking place

Broken SSL sessions displaying unencrypted third party content, allow active tracking and monitoring to take place as well

Forcing a full-session on a popular social networking service such as Facebook for instance, without taking into consideration the fact that SSL would not magically make all the personally identifiable information, including your IP, disappear, is wrong. Full-session SSL, in combination with tools such as [Vanish](#) (see a [related video](#)), next to Tor-like/VPN based anonymity network, are great for a fresh start

It's great to see that [the EFF is also emphasizing](#) on the insecure third-party content issue:

As always, even if you're at an HTTPS page, remember that unless Firefox displays a colored address bar and an unbroken lock icon in the bottom-right corner, the page is not completely encrypted and you may still be vulnerable to various forms of eavesdropping or hacking (in many cases, HTTPS Everywhere can't prevent this because sites incorporate insecure third-party content).

UPDATED: EFF's Peter Eckersley elaborates on HTTPS Everywhere extension:

Our original design objective was to offer an easy way to encrypt all Google searches; once we'd done that we realised we could support a lot of other useful sites too. We had to implement several things that NoScript STS lacked, including:

- **Rewriting rules** , so that a search at google.ch (for example) gets rewritten to <https://www.google.com/search?hl=<lang>>, because there is no https support at google.ch. URL reconstruction was also necessary for Wikipedia.
- **Detect loops** when some page on an https:// site redirects back to http:// (parts of Facebook's privacy settings do that, for example!). Currently we just render the http:// page when that happens, though we're planning to offer a setting that turns those into error conditions.
- **Support exclusions** if *.domain.com supports https with one or two subdomains as weird exceptions.

We think that the result is something that's useful on its own, as a simple way to move a lot of traffic to https, but also something that offers useful new functionality even if you already use NoScript. We also hope that some of these improvements can be patched back into NoScript; but for the time being we'll keep offering a tool that offers them and is also useful to people who don't yet have the sophistication to manage all of NoScript's features.

What's worth pointing out is that, [forced SSL connections](#) ([STS](#) support in both, [NoScript](#) and HTTPS Everywhere), as well as the additional security added by [Secure Cookie Management](#), has been an integral part of the NoScript Firefox extension.

In a way, EFF's "HTTPS Everywhere" is a user-friendly version of NoScript's forced SSL feature, which is a step in the right direction,

given the number of people that will definitely start taking advantage of it.

Personally, I'm sticking with [NoScript's](#) forced SSL, and Secure Cookies Management for now. And you?

Talkback.

The cyber security implications of Iran's government-backed antivirus software | ZDNet

According to [independent media reports](#), Iran has [banned the import of foreign security software](#), and has been secretly working on its own antivirus solution since 2010.

Developed by Iranian experts from Shiraz Computer Emergency Response Team of APA (Academic Protection and Awareness), the software has undergone active testing and is ready to be used on government and military installations.

Key points to consider:

The U.S, Russia and China are developing offensive cyber warfare weapons -- weaponized malware -- successfully bypassing the most popular antivirus solutions. Will Iran undermine the effectiveness of these cyber weapons? - not necessarily. What Iran's decision to rely on a government-backed antivirus software will do, is increase the interest of foreign governments into obtaining and analyzing the software on their way to exploit vulnerabilities in its design for the purpose of successfully bypassing it in the long term. Until access to the software is obtained, it will definitely undermine QA (quality assurance) practices aiming to ensure that the weaponized malware is not detected by popular antivirus vendors.

Reliance on largely untested in-house built software in comparison to outsourcing to vendors with decades of experience is a flawed strategic approach - Iran's adversaries should be thankful for Iran's largely flawed approach to secure the nation's infrastructure from malicious code. Instead of importing innovative solutions, and embedding multiple antivirus solutions to protect endpoints, the country's nationalist sentiments seems to be prevailing, potentially exposing the country's infrastructure to malicious attacks.

Basing your entire strategy on a single endpoint solution,

undermines the concept of defense in-depth - Iran doesn't seem to be aware of the defense in-depth concept, ensuring multi-layered approaches to securing a network or an endpoint system. The country's ban on foreign security products, mean it will have to build firewalls, intrusion prevention/detection systems from scratch, in complete isolation from the rest of the industry. This will result in major flaws in the design and actual applicability of these in-house built products.

From an Information Warfare perspective, by banning foreign imports of security products, Iran might be setting the foundations for a successful self-mobilizing cyber militia campaign - Antivirus tools don't just detect viruses, they detect malicious code in general such as DoS (denial of service) attack and DDoS (distributed denial of service attack) tools. In case of a cyber conflict, relying on the basis of Information Warfare, Iran could distribute software agents to civilians in order to use their bandwidth or Internet connectivity in general for waging Information Warfare. We've seen this happen on numerous occasions in the past. In event of a cyber conflict, Iran's antivirus software could on purposely skip the detection for these malicious tools that would otherwise be detected by foreign antivirus software in an attempt to ensure that the Iranian population will participate in the cyber conflict. See: [Attack of the Opt-in Botnets](#)

Moreover, Iran's antivirus doesn't participate in any of the industry comparative reviews performed on a periodic basis evaluating the effectiveness of antivirus software, it doesn't participate in chapters of such organizations such as the Honeynet Project, it doesn't share samples with competing vendors, and it doesn't require them to share samples in the same way. This self-serving mentality typical for communist regimes, will ultimately allow foreign adversaries easy access to Iran's infrastructure, and in particular to hosts running the largely untested antivirus software.

Diversification may results in complexities which on the other hand result in insecurities, but basing the protection of endpoints on a single, largely untested product, results in monocultural insecurities posed by the use of a single, potentially 'buggy' product.

Iran isn't the first [country to start developing its own hardened security products](#), however it's among the few to ban imports of foreign security software on the local market. China with its Red Flag Linux and Kylin OS, the European Union with its secure [OS Minix](#), and Russia which also [expressed interest in the concept](#), are among the countries that are considering to migrate from using U.S developed Operating Systems in order to migrate from the monocultural insecurities posed by the world's most popular Operating System - Microsoft's Windows.

What do you think? Is Iran's move putting the U.S, Russian or China at a strategic disadvantage, or is the move largely exposing Iran's infrastructure to amateur malware authors who will inevitably start bypassing Iran's proprietary antivirus software?

TalkBack.

Find out more about Dancho Danchev at [his LinkedIn profile](#), or [follow him on Twitter](#).

The current state of the crimeware threat - Q&A | ZDNet

With [Zeus crimeware infections](#) reaching epidemic levels, [two-factor authentication under fire](#) , and the actual [DIY \(do-it-yourself\) kit becoming more sophisticated](#) , it's time to reassess the situation by discussing the current and emerging crimeware trends.

What's the current state of the crimeware threat? Just how vibrant is the underground marketplace when it comes to crimeware? What are ISPs doing, and should ISPs be doing to solve the problem? Does taking down a cybercrime-friendly ISP has any long term effect?

I asked [Thorsten Holz](#) , researcher at Vienna University of Technology, whose team not only participated in the recent [takedown of the Waledac botnet](#) , but [released an interesting paper](#) earlier this year, summarizing their findings based on 33GB of crimeware data obtained from active campaigns.

Go through the Q&A.

Dancho: Were you surprised that you were able to extract the data from the crimeware dropzones, so easily? Given the quality assurance practices that these people often put into their campaigns, it's logical to assume that they've taken basic precautions on the server/kit level.

Are cybercriminals taking the operational security of their campaigns seriously?

Thorsten: Actually I was rather surprised that we found so many open dropzones, it seems like the attackers do not follow security best practices. Especially earlier versions of Nethell had very often an open directory where all log files could be found by simply browsing to the correct URL. For ZeuS, we found only a handful of open dropzones, it seems like the attackers using that toolkit have more clue about what they are doing. Unfortunately, this has changed in the recent months: by now, most dropzones are

configured correctly by default and thus it is not common anymore to find open dropzones.

Dancho: Considering the fact that security researchers are clearly capable of extracting campaign data, it's fairly logical to assume that cybercriminals are also peeking into each other's botnets, Zeus in particular.

Do you agree or disagree?

Thorsten: Yes, that definitely makes sense. Presumably an attacker can also use other methods to access a dropzone from another attacker: an attacker could exploit vulnerabilities in the dropzone's web app (e.g., SQL injection, default passwords, open MySQL access etc.), something that we could not do as part of our research. There have been some reports about vulnerabilities in dropzone kits, and I am sure that one could find other ways to access a dropzone.

Dancho: With Zeus clearly reaching a monocultural stage within the cybercrime marketplace, a remotely exploitable flaw within the kit's web interface could trigger an effect often seen from a white hat's perspective. In fact, there have been cases of cybercriminals hijacking one another's Zeus botnet due to insecurely configured web servers.

Do you believe these are isolated incidents, or a logical development in the long term, which could contribute to the rise of underground turf wars?

Thorsten: I think that this is a logical development: If I would be an attacker, it would be way easier to simply exploit other dropzones than doing all the hard work on my own (buying the kit, hosting it, exploiting machines etc.). And with tools such as Zeus Tracker I could also easily find other dropzones and perform my attack on a larger scale.

Go through related posts on the Zeus crimeware: [Zeus Crimeware as a Service Going Mainstream](#) ; [Modified Zeus Crimeware Kit Comes With Built-in MP3 Player](#) ; [Zeus Crimeware Kit Gets a Carding Layout](#) ; [The Zeus Crimeware Kit Vulnerable to Remotely](#)

[Exploitable Flaw ; Help! Someone Hijacked my 100k+ Zeus Botnet! ; Inside a Zeus Crimeware Developer's To-Do List](#)

Dancho: Since not every cybercriminal is willing to invest money into purchasing the very latest Zeus release, hundreds of them continue using old releases while continuing to update the "Web Injections" list.

A few months ago, based on an observation of ongoing discussions on the topic, I became aware of the fact that certain cybercriminals are in fact attempting to use the ZeusTracker to build hit list of potentially exploitable targets.

A trend, a fad, or someone's basically scratching the surface here?

Thorsten: I see this as a trend: since the information is freely available, it makes sense from an attacker's point of view to take advantage of it. Presumably it requires only some coding effort to crawl Zeus Tracker, extract the info about the dropzone, and then probe it for open access or vulnerabilities.

[Managed crimeware services, or raw crimeware logs as a service?](#)

-->

Dancho: Embracing the Cybercrime-as-a-Service model, opportunistic cybercriminals have been offering managed crimeware services for a few years now. In fact, some of the services truly demonstrate the dynamics of the cybercrime ecosystem by offering items that were once exclusive, now a commodity, as a bonus for extended use of the crimeware service.

In between, there's another no so well publicized market segment that's becoming a rather popular business proposition these days. It's the actual sale of gigabytes of raw crimeware/accounting data based on a recent period of time, or for a particular country only, with the customer not even having to rent access to a managed crimeware service.

Do you think the sale of raw crimeware data will surpass the growth of managed crimeware services in general? Is quantity proportional to quality in this case, and does this developing

market segment makes it even easier for novice cybercriminals to obtain access to raw crimeware logs?

Thorsten: Yes, I also noticed this when studying underground boards/channels. However, I am not sure about this: if you buy raw logs, you can not be sure if you obtain some interesting info or only junk. As an attacker, I would prefer to target specific people and try to collect "interesting" data. Raw logs can contain surprising info, but you can also not be sure whether the seller removed interesting data such as credit card numbers, or if the seller has already abused the stolen credentials (which then lowers its value).

Dancho: Over the past year, cybercriminals have started monetizing the actual buzz surrounding web malware exploitation kits, and banking malware in general, by backdooring and releasing for free copies of these kits, proving that there's no such thing as a free malware kit, unless of course it's backdoored.

How big do you think is the potential of a underground model where potential cybercriminals unknowingly allow the sophisticated/opportunistic ones to harvest the data they were able to aggregate, in between forwarding the responsibility for maintaining the botnet/campaign to the novice cybercriminal?

Thorsten: Yes, an addition to the famous [Mr. Brain phishing kit backdoors](#) . In the phishing world this model works pretty well, see the study by my colleagues from UCSB. I think this could also easily work for dropzones and other types of web-based exploit kits. If an attacker puts some effort into hiding his backdoor in the code, then it might be undetected for some time. And again it is an easy way for an attacker to obtain stolen data: instead of setting up the whole campaign on his own, he just has to put some effort into hiding the backdoor.

Dancho: There are now web malware exploitation kits, which include a "seller module" allowing the cybercriminal to rent access to, or manage separate campaigns for other people. Do you believe that these kits would inevitably mature from today's tool for exploitation, to tomorrow's cybercrime-facilitating platform?

Thorsten: This definitely has potential to become a trend. Renting the whole platform for some time or only for specific campaigns actually makes sense: perhaps an attacker just wants to have some credentials for specific services and thus he can avoid the overhead by renting a framework. I expect that this kind of "service" will continue to expand.

Consider going through related crimeware posts: [Modern banker malware undermines two-factor authentication](#) ; [Report: 48% of 22 million scanned computers infected with malware](#) ; [Crimeware tracking service hit by a DDoS attack](#)

Dancho: It's a "public secret" that thanks to quality assurance services within the cybercrime ecosystem, signature-based scanning is easily bypassed, and on the majority of occasions the people behind the campaigns would even measure the detection rate of their binaries before releasing them in the wild. The process is, of course, entirely automated and cost-effective from a cybercriminal's perspective.

Thorsten: Some researchers also built such a system - ["PolyPack" is a research project](#) at the University of Michigan aimed at understanding the impact of malware packers on modern antivirus products.

PolyPack highlights the failure of signature-based antivirus against common, widely available packers, investigates the role that diversity plays in the capabilities of both the packers and antivirus engines, and demonstrates the ease and efficacy with which an attacker could deploy an online packing service for nefarious purposes in a deployment model known as crimeware-as-a-service (CaaS).

The PolyPack web service uses an array of packers and antivirus engines to evaluate the effect that each packer has on the detection capabilities of the antivirus engines. Our current implementation employs 10 of the most common packers observed in the wild and 10 popular antivirus engines. A submitted binary is packed by each of the 10 packers and then analyzed by each of the 10 antivirus engines. The details of a few example results are available to the public."

[On TROYAK's takedown, and crimeware fighting strategies](#) -->

Dancho: Where do you see the gap between the epidemic growth of crimeware, and the average end user's awareness still orbiting around perimeter defense solutions such as antivirus, or the practice of excluding client-side vulnerabilities from the big picture?

Thorsten: [Going through related articles](#) , it becomes clear that AV is definitely behind the latest attacks and it is no surprise that we see a prospering underground ecosystem.

While the user awareness is rising due to media attention and everything, I think that we still need to do some work in that area: users need to understand that the Internet is not always a safe place and that they need to be responsible when surfing the web. Security best practices like regular patching or not clicking on everything are not followed by many, I think that's definitely an area that we need to improve.

Dancho: What's worse in this situation? The reactive, post-infection awareness building process, or the false feeling of security offered by two-factor authentication tokens with the end user unaware of the fact that their sessions are hijacked on-the-fly each time they interact with their E-banking provider?

Thorsten: That's a good point! Security solutions can not protect you against everything, a two-factor authentication on a compromised machine does not help much. People will learn due to security incidents, but the process can be a pain and the attackers always have some reward.

Consider going through related posts: [Citizens Financial sued for insufficient E-Banking security](#) ; [Commonwealth fined \\$100k for not mandating antivirus software](#) ; [No security software, no E-banking fraud claims for you](#)

Dancho: Over the past week, the cybercrime-friendly TROYAK-AS has been struggling to remain online despite numerous attempts to take it down.

How beneficial are these takedowns in the long, and in the short term, considering the fact that the industry and the

cybercrime ecosystem are both, in a "learning mode" of each other's tactics?

Thorsten: That's actually a good question and I have already spent quite some time with discussions on the subject. Taking down a cybercrime-friendly AS or taking down botnets such as Waledac always has two facets: on the one hand, it is good to do this since we can then stop to crime operation and the criminals can then not abuse the infected machines anymore. Side-effects such as spam, credential stealing and similar malicious actions then also stop. On the short run, it is thus good since we make the life of the attackers harder.

Recommended reading: [TROYAK-AS: the cybercrime-friendly ISP that just won't go away](#) ; [AS-Troyak Exposes a Large Cybercrime Infrastructure](#)

On the other hand, there are also reasons not to stop malicious AS or not to take down botnets: we loose some precious insights. When shutting down TROYAK-AS, many ZeuS servers went offline, but the attackers do presumably not stop doing their stuff: they will simply move to another hoster, continue the operation, and learn their lessons to stay under the radar longer next time. Thus we force an arms-race and force the attackers to evolve.

At the same time, the defenders need to closely follow the attackers: previously, we knew that many ZeuS server were hosted at TROYAK and could study them (perhaps also together with the police, in order to track down the actual attackers). Now we need to search for new locations and update our knowledge, such that we can follow the attackers again. On the long run, this kind of takedown actions thus forces an arms race and evolution at the attacker's side.

Dancho: Also, which practice do you think should get more priority in the long term? Shutting down the botnets, going after the ISPs, or putting more efforts into going after the individuals behind these campaigns?

My point - the Internet can be a pretty small place if you can get international law enforcement agencies, private sector companies and the academic community to start constructively sharing data, and prioritizing the gangs/incidents.

Thorsten: Going after the actual individuals who run the botnets ([Police arrest Mariposa botnet masters, 12M+ hosts compromised](#)) would be the best approach: only when we can catch them, they will stop doing harm. A good example here is the group behind Storm Worm: they had built an interesting, peer-to-peer based botnet that was rather successful and infected hundreds of thousands of machines (presumably also making quite some cash).

When Storm was shut down, it did not take too long and Waledac appeared: the malware has evolved, but many of the concepts stayed the same (e.g., spam template language). Waledac was recently shut down and the attackers can not send commands to the infected machines anymore.

However, I expect that we see a new, evolved attack by the same group in the near future since they will presumably not stop doing their harm. Instead, they will likely find new ways to make the botnet more robust next time. Unfortunately, going after the attackers is a tough task: collaboration among international law enforcement agencies can take some time, there is also lots of bureaucracy involved. But if we collaborate, I think this would definitely improve the overall situation.

[Pros and cons of disconnecting malware-infected customers from the Internet](#) -->

Dancho: Whether a cybercrime-friendly ISP goes down or not, cybercriminals proved that they have the contingency planning in place to continue their malicious operations elsewhere.

Has the time come for ISPs (Internet Service Providers) to start disconnecting malware-infected customers from the Internet, instead of basically notifying them that they're infected?

Thorsten: Disconnecting is presumably not an optimal solution and I expect that not many ISPs will do this. After all, the customers will definitely not like this, the ISP do not have much incentive to do this, and ISPs also often do not have the necessary expertise/infrastructure to detect infections. There could also be legal caveats prohibiting ISPs to do this, after all they are typically only

providing the service and they need to make sure that the customer can reach the network.

Notifications would be nice, [I hope that more ISPs adopt this model](#) in the future and finally start to do something. After all, they are in a good position to do this - perhaps some legal ruling would help here, forcing ISPs to pro-actively adopting some security mechanisms. Actually some German ISPs plan to build such a system, the government will also support this. I think this is a step in the right direction, let's see how such a systems works in practice.

Dancho: Having an active cybercrime-friendly ISP is one thing, but having it online with no bots connecting to it since their ISP disconnected them is entirely another.

Virtually, it undermines a huge percentage of the services currently offered within the cybercrime ecosystem.

What do you think?

Thorsten: But it also has some drawbacks: why would an ISP do this (if not force by some laws)? For an average user who can choose between an ISP that disconnects him when his machine is compromised and an ISP who takes no action, the customer will presumably choose the latter.

I know that there are good reasons to disconnect infected machines, but I am not sure whether this will get wide-spread adoption in the near future. Some ISPs have implemented Walled Gardens such that they can separate infected machines and inform the user, perhaps some more ISPs adopt that model.

Dancho: In conclusion, are you optimist, a pessimist, perhaps even a realist in respect to solving the crimeware problem, once and for all?

Thorsten: As a researcher, I am an optimist that we will solve some of the problems and come to good solutions for some of the current problems. Taking a look 10 years back: we had Windows 98 and Windows 2000 has been released. Compared to Windows 7, we now have some huge improvements and I hope that we can say the same in 10 years when we have better operating systems and detection mechanisms.

But I am also a little realist: we will not solve everything and the "human factor" will still be a problem in the future. Social engineering tricks will presumably always work and threats like rogue AV solutions highlight this aspect: many people well for these tricks and the attackers made a small fortune out of rogue AV.

'The Creator of LulzSec arrested in London' scam spreading on Facebook | ZDNet

Researchers from Sophos are reporting on a [currently circulating viral Facebook scam](#), *'The Creator of LulzSec arrested in London (PHOTO TAKEN BY THE POLICE)'*.

Spamvertised as:

The Creator of LulzSec arrested in London (PHOTO TAKEN BY THE POLICE) SEE THE PICTURE WITHOUT BLURRING, SHARE THIS PAGE AND LIKE IT !!

Once the socially-engineered users -- event-based social engineering tactic -- click on the link, they're offered the option to like and share the picture in order to view it. In reality though, the scammers are monetizing the campaign by pushing the **iLividSetupV1.exe** executable which drops several toolbars on the infected machine, with the scammers earning revenue each and every time the toolbars get installed.

Targeted Pro-Tibetan malware attacks hit Mac OS X users | ZDNet

According to a newly published data, [Mac OS X users are just as susceptible to targeted attacks](#), as Windows users are, thanks to the emergence of popular tactics within the cybercrime ecosystem known as [localization, market segmentation, and event-based social engineering attacks](#).

What's particularly interesting about this campaign, is the fact that the [same C&C server](#) used in it, was also [observed](#) in [recent targeted attacks](#) observed by [AlienVault Lab](#).

This is the second Tibet-themed targeted malware attack intercepted for March, 2012, following the one researchers from [AlienVault Lab uncovered earlier this month](#).

The malware is currently detected as TROJ_MDROPR.LB.

Targeted malware attacks exploiting IE7 flaw detected | ZDNet

Researchers at [TrendMicro](#) have detected a targeted malware attack exploiting last week's patched [critical MS09-002 vulnerability affecting Internet Explorer 7](#) . Upon opening the spammed Microsoft office document, vulnerable users are automatically forwarded to a Chinese [live exploit site](#) which still [remains active](#) .

The attack has also been [confirmed by McAfee](#) and [by the ISC](#) , who point out that the cybercriminals appear to have reverse engineered Microsoft's patch in order to come up with the exploit.

From TrendMicro's post:

The threat starts with a spammed malicious .DOC file detected as XML_DLOADR.A. This file has a very limited distribution script, suggesting it may be a targeted attack. It contains an ActiveX object that automatically accesses a site rigged with a malicious HTML detected by the Trend Micro Smart Protection Network as HTML_DLOADER.AS.

HTML_DLOADER.AS exploits the CVE-2009-0075 vulnerability, which is already addressed by the MS09-002 security patch released last week. On an unpatched system though, successful exploitation by HTML_DLOADER.AS downloads a backdoor detected as BKDR_AGENT.XZMS.

This backdoor further installs a .DLL file that has information stealing capabilities. It sends its stolen information to another URL via port 443.

The attackers trade-off in this case is to either launch a less noisy targeted attack, or attempt to target as many users as possible by using legitimate web sites as infection vectors, a choice that depends on what they're trying to achieve, and who are they targeting in particular.

Who's behind the attack anyway? The web service (**9966.org**) used as a "phone back" location with the stolen data, is a well known

one used primarily by Chinese hackers in previous massive SQL injections attacks, which doesn't necessarily mean the campaign is launched by Chinese hackers, since it could be international hackers from anywhere using a well known malicious infrastructure in order to forward the responsibility to local hackers.

Moreover, in this particular campaign I can easily argue that the window of opportunity for abusing this vulnerability in a targeted fashion, is just as wide open as [attempting to exploit the same hosts by diversifying the use of different exploits](#) . For instance, despite the timely exploitation of MS09-002, based on the [number of Conficker affected hosts globally](#) , a situation where once again a patch is present, there's a great chance that some of the hosts they're attempting to exploit through the use of MS09-002 are already part of Conficker's botnet, or remain susceptible to outdated vulnerabilities.

So far, no massive malware campaigns are taking advantage of the exploit, but users are advised to [self-audit themselves](#) against known client-side vulnerabilities and [MS09-002](#) in particular.

Targeted malware attack against U.S schools intercepted | ZDNet

Timing is everything, and from a cybercriminal's perspective, a new school year means segmenting their email databases to launch a targeted attack welcoming everyone back online. According to [MessageLabs Intelligence](#) :

"Starting in early September, MessageLabs intercepted a targeted, email-borne malware attack on US schools and government organizations, a majority of which are located in New Mexico, Virginia, Illinois and Hawaii. The attack comprised more than 1000 emails from only 15 source IP addresses, most of which were located in the former Soviet Union on consumer-based address ranges signaling that the attacks are the result of a botnet that may be looking to expand. The attached table illustrates the distribution of mails intercepted from the source IP addresses used in the attack."

Naturally, the attackers are taking advantage of already infected with malware hosts, and using them as stepping stones for launching the attacks ending up in anecdotal cases where U.S based infected hosts are used to launch targeted attacks against U.S schools and organizations.

Some more details on the specifics of the attack :

"Analysis reveals that dispersement lasted almost two days and used social engineering techniques to deliver the malware, Trojan-Spy.Win32.Zbot.ele, as both an executable email attachment and a link within an email, disguised as a Microsoft Windows Update. There were three similar attacks targeting US schools, businesses and state governments. According to MessageLabs, these attacks may be deploying the Antivirus XP 2008 malware."

As of recently, cybercriminals are putting more efforts into the quality assurance of their campaigns by means of localizing the spam message to the native language of the receipts, known due to the segmented email database belonging to a particular sector that they've already purchased. However, in this particular targeted

attack they seem to have underestimated the personalization of the emails, and despite the obvious segmentation of potential victims to spam, were taking advantage of average social engineering tactics more suitable for a large scale malware campaign.

The much more sophisticated from a social engineering perspective variant of this targeted attack, is spear phishing, which [according to iDefense is increasing](#) , with a few groups specializing into targeting high-profile targets :

"The victim counts from these attacks is staggering – over 15,000 corporate users in 15 months. Victims include Fortune 500 companies, government agencies, financial institutions and legal firms. In these attacks, the goal is to gain access to corporate banking information, customer databases and other information to facilitate cyber crime. Two groups of attackers have carried out 95 percent of these attacks."

Earlier this month, [South Korean officers were also reportedly under a targeted attack](#) from North Korean hackers that managed to obtained the personal emails of the officers thanks to a "real life email harvester" collecting name cards with the emails on them, and spam them with malware :

"A North Korean spyware e-mail was reportedly transmitted to the computer of a colonel at a field army command via China in early August. The e-mail contained a typical program designed automatically to steal stored files if the recipient opens it. Some officers whose email addresses are on their name cards have suffered hacking attacks."

What's important to note is that in such cases a high-profile victim's personal email address can easily turn to be the weakest link in an ongoing espionage campaign against a particular country, where despite that the adversaries aren't capable of breaching their private emails, the ongoing and previous conversations found in their personal ones could contribute to real-life espionage attempts against them.

In times when phishers, spammers and malware authors are consolidating, it is logical to assume that targeted attacks will only get more personalized and well crafted in the very short term.

Targeted attack against UAE activist utilizes CVE-2013-0422, drops malware | ZDNet

Earlier this month, [BahrainWatch.org](#) was contacted by an UAE activist, who reported receiving a suspicious email. Upon deeper examination, it was revealed that it was a targeted attack relying on Java exploit ([CVE-2013-0422](#)), which would have dropped a Remote Access Trojan (RAT), if the attack hadn't been detected.

The malware was hosted on the isteeler(dot)com domain, which on November 9, 2012, was registered with the following email: brightjam@163.com, ultimately dropping [MD5: e5dc7ecfc5578d51ba92ff710b05ae09](#) on the affected hosts. Upon execution, the sample phoned back to storge(dot)myftp(dot)org:15999 (109.169.17.234). The malware marks its presence on the affected host in the following way: `[HKEY_CURRENT_USER\Software\DAMAR]; NewIdentification = "DAMAR"`.

This isn't the first time that [government-tolerated cyberespionage actors target UAE activists](#), and definitely not the last. What's particularly interesting about this incident is the fact that, those who orchestrated it didn't rely on lawful interception tools, like [the German government](#) does on the majority of occasions. Instead, they relied on a modified version of a well-known RAT, a practice that combined with the use of easily obtainable malware crypters, could completely bypass a host's signatures-based antivirus protection in place.

There's another aspect of these cyberespionage campaigns, worth considering in the context of the big picture. It's the practice of data mining already infected hosts, with the idea to [use them as sources of intelligence](#). Basically, a huge percentage of the population with restricted Internet access in a country under a totalitarian regime, could be controlled by either using publicly obtainable tools, or by actually purchasing [access to malware-infected hosts within this](#)

[country](#) in a cost-effective way compared to using lawful interception tools, and deploying them.

What do you think--is cyberespionage against activists and dissidents the work of government-funded units, or was cyberespionage actually privatized years ago, leading to anything else but actual results and a pay check?

Find out more about Dancho Danchev at his [LinkedIn profile](#) .

Taiwan busts hacking ring, 50 million personal records compromised | ZDNet

Taiwan's [Criminal Investigation Bureau \(CIB\)](#) has successfully tracked down and arrested six people in what the CIB

believes to be the [biggest personal data breach in Taiwan](#) to date. Apparently, the group also managed to obtain personal data on Taiwan's current and former presidents :

"The suspects are believed to have stolen more than 50 million records of personal data, including information about President Ma Ying-jeou, his predecessor Chen Shui-bian and police chief Wang Cho-chiun, the official said. They then offered to sell the information for 300 Taiwan dollars (10 US) per entry, he said. The hackers, based in Taiwan and China, also swindled victims out of millions of Taiwan dollars through their online bank accounts, he said."

The announcement comes a week after [China detected a sophisticated fake diploma scheme](#) , where ten government databases were compromised.

This particular data breach seems to very similar to the "whether to attack the bank or its customers as the weakest link" dilemma malicious attackers used to face once. Basically, the same amount of information can be obtained by targeting the weakest link, in this case the end users, whose once crimeware infected hosts ends up in a cybercrime as a service underground proposition. [Take for instance the 76service](#) , which recently reappeared as an alternative for cybercriminals not wanting to take the time and effort to build botnets, but still wanting to rent one and intercept all the personal and financial information they can during the a particular period of time. With geolocation within botnet for hire services now a daily reality, someone interested in intercepting data from a particular country only, can easily do so.

As for the people behind this hacking ring, asking for 10 USD per data entry clearly indicates their isolation from the underground marketplace, as in reality, what they are offering may already be

available somewhere else in a wholesale proposition, or requested on demand at a cheaper price.

Swine flu email scams circulating | ZDNet

Opportunistic scammers and [spammers](#) are actively exploiting the swine flu buzz across the web by spamvertising links to pharmaceutical scams, and bogus 'Swine Flu Survival Guides' using search engine optimization of [typosquatted domains related to the outbreak](#) .

The event-based social engineering campaign is similar to the recent fake '[Conficker infection alerts](#) ', the [bogus Conficker removal tools](#) pushed through SEO practices, and the timely spam campaign serving malware as a [fake Microsoft patch Tuesday message](#) .

Strangely, the massive spam campaign doesn't seem to be targeting the specific market segment since upon clicking on the links the users are directed to the ubiquitous Canadian Pharmacy scam. Based on previous experience with related campaigns, cybercriminals are prone to diversify the traffic acquisition tactics, so consider keeping yourself informed on the issue by [using the right sources](#) .

This isn't the first time that viral outbreaks are being used by cybercriminals in order to increase the trust factor of a particular campaign. According to Trend Micro's researcher **Ivan Macalintal** , a similar event-based spam campaign took place in 2003 in the wake of the SARS epidemic with the [mass-mailing Coronex worm](#) campaign using SARS related messages to spread.

The bottom line - [don't bargain with your health](#) , and drive the cybercrime economy in between.

Survey: Millions of users open spam emails, click on links | ZDNet

How many users access spam emails, click on the links found within, and open attachments intentionally? Why are they doing it, and who are they holding responsible for the spread of malware and spam in general, in between conveniently excluding themselves?

A newly released [survey from the Messaging Anti-Abuse Working Group \(MAAWG\)](#) , summarizing the results of the group's second year survey of email security practices, offers an interesting insight into the various interactions end users tend to have with spam emails.

Key findings of the survey:

Nearly half of those who have accessed spam (46%) have done so intentionally – to unsubscribe, out of curiosity, or out of interest in the products or services being offered

Four in ten (43%) say that they have opened an email that they suspected was spam

Among those who have opened a suspicious email, over half (57%) say they have done so because they weren't sure it was spam and one third (33%) say they have done so by accident

Canadian users are those most likely to avoid posting their email address online (46%). Those in the U.S., Canada and Germany are most likely to set up separate email addresses in order to avoid receiving spam

Many users do not typically flag or report spam or fraudulent email

When it comes to stopping the spread of viruses, fraudulent email, spyware and spam, email users are most likely to hold ISPs and ESPs (65%) and anti-virus software companies (54%) responsible

Less than half of users (48%) hold themselves personally responsible for stopping these threats

It's interesting to see the paradox of end users blaming ISPs and antivirus vendors, whereas 43% of the surveyed users said that they

have accessed spam emails, and that they do not typically flag or report these emails.

What the majority of the survey participants appear to be unaware of, is that, despite the fact that since early days of spam, [spammers have been attempting to verify the validity of the emails](#) using DIY tools, **on their way to unsubscribe themselves, the users are actually confirming that their email is valid .**

In short, it means even more spam.

Go through related posts: [From Russia with \(objective\) spam stats](#) ; [Spamming vendor launches managed spamming service](#) ; [Phishing experiment sneaks through all anti-spam filters](#) ; [Inside an affiliate spam program for pharmaceuticals](#) ; [Inside a DIY Image Spam Generating Traffic Management Kit](#)

Moreover, the survey indicates that a common misunderstanding among end users, is still dominating their perspective of spam in general. Nowadays, spam is no longer a mass marketing channel for counterfeit goods/pharmaceuticals only.

Spam is both, an infection and propagation vector for malware campaigns in general, with an interesting twist - the most aggressive [Zeus crimeware serving campaigns for Q1, 2010](#) , were optimizing the traffic they were getting through the spam campaigns, by embedding client-side exploits on the pages, next to actual malware left for the end user to manually download and execute.

The most extensive study of end user's interaction with spam emails, was conducted in 2008 ([Spamalytics: An Empirical Analysis of Spam Marketing Conversion](#)), showing that users not only click on spam links, but that they're actually buying dangerous counterfeit pharmaceuticals:

After 26 days, and almost 350 million email messages, only 28 sales resulted -- a conversion rate of well under 0.00001%. Of these, all but one were male-enhancement products and the average purchase price was close to \$100. Taken together, these conversions would have resulted in revenues of \$2.731.88 -- a bit over \$100 a day for the measurement period or \$140 per day periods when the campaign is active. Under the assumption that our

measurements are representative over time (an admittedly dangerous assumption when dealing with such small samples), we can extrapolate that, **were it sent continuously at the same rate, Storm-generated pharmaceutical spam would produce roughly 3.5 million dollars of revenue in a year.**

What do you think? Why are users still interacting with spam emails, which could easily lead them to drive-by exploits serving web site? Are ISPs or vendors to blame, or the end user's lack of awareness on the risks involved when interacting with spam emails these days? Do you think that spam is fought in the wrong way, in the sense that before it reaches your Inbox, it has to go out from the network of a socially-irresponsible ISP first?

Talkback.

Survey: 88% of Mumbai's wireless networks easy to compromise | ZDNet

Deloitte's recently released [Wireless Security Survey assessing Mumbai's](#) -- India's financial capital -- state of security awareness in respect to wireless security, shows an ugly picture of insecure wireless networks in both, business, and residential districts. With Mumbai being the home of [India's most important financial institutions](#), next to the majority of multinational corporations, it may also turn into the playground for the next high profile data breach.

The key findings of the survey are:

Of the 6729 wireless networks seen, 36% appeared to be unprotected i.e. without any encryption

52% were using low level of protection i.e. Wired Equivalent Privacy (WEP) encryption

Over 95% of the networks broadcast their SSID, with 25% of these using their router's default SSID

Balance 12% were using the more secure Wi-Fi Protected Access (WPA)

What's the practical applicability of these insecurities?

Last week, it became evident that a group of Indian militants [took unethical hacking courses](#), and once learning the basics of wardriving, used the [insecure wireless network of a U.S expatriate](#) to send [emails claiming responsibility](#) for serial bombings that took place in July and September :

"Roaming around Mumbai with Wi-Fi detectors, the suspects looked for open Wi-Fi signals and programmed the e-mail messages to be sent from hacked wireless networks prior to the blasts, the Indian police said. The technique used by the militants is similar to "wardriving," where hackers roam around to detect and access Wi-Fi networks with security weaknesses.

They would roam in a car to sites where wireless internet was available and then send the emails at designated timings, he said. "The police have seized a laptop, six computers, a radio frequency

detector, a wireless router, anesthetic injections and tablets from the trio," said Gaffoor. Mohammed Akbar Ismail Chaudhary, the driver of the vehicle in which they travelled to send the threatening emails, has also been arrested. "Chaudhary had taken a house in Surat on rent under a fictitious name prior to planting bombs there," said Maria."

And whereas Deloitte didn't attempt to verify whether or not the wireless networks with default SSIDs were also using the [default router passwords](#) , that may well be the case as well. Living in Mumbai or not, consider going through the [WiFi Security Awareness booklet](#) accompanying the survey.

Sadly, Mumbai isn't an exception to the overall rule that best practices supposed to have been implemented, are not, since the same lack of basic security awareness can be seen literally all over the world - [Caracas \(Venezuela\)](#) ; [London](#) ; [Paris](#) ; [China](#) ; [Monterrey — Mexico](#) ; [Sao Paulo – Brazil](#) ; [England](#) ; [Germany - CeBIT2006](#) ; [Warsaw](#) .

Survey: 60 percent of users use the same password across more than one of their online accounts | ZDNet

How often do you change your password? Do you share your passwords with family members, and how confident are you that malicious attackers wouldn't be able to guess your password?

According to a [newly published survey results](#), 60 percent of users use the same password across more than one of their online accounts.

More findings from the survey which sampled 1000 Australians:

Over three quarters (77%) of Australians have more than three online passwords

Nearly all (90%) of Australians are confident others wouldn't be able to guess their online passwords

Nearly two thirds (60%) of Australians use the same password across more than one of their online accounts

Almost half (48%) of Australians only change their password when required to by a system

Nearly half (42%) of Australians have shared their password with a friend, family member or work colleague

Over a third (36%) remain logged into their online accounts

Nowadays, cybercriminals rarely brute force their way into a user's account, even though the [CAPTCHA-solving process can be easily outsourced](#). Instead, they rely on data mining of malware-infected hosts for stolen credentials. The data is later on used for spreading of malicious code, or for active spamming purposes.

Just how important is to change your passwords regularly? Depends on the perspective. Whereas the more often you change a password, the higher the probability that a malicious attacker that's actively data mining botnets, will be left with outdated data, changing your password on a malware-infected host is pointless, as the

malicious attacker would once again obtain access to your accounting data.

Go through related posts:

[And the most popular password is... Weak passwords dominate statistics for Hotmail's phishing scheme leak Study: password resetting 'security questions' easily guessed](#)

How do you deal with your passwords overload? Do you write them down, or conveniently store them in digital format? How often do you change them, and do you use the same password across multiple web properties? Do believe that strong passwords in a world dominated by malware infected hosts are worth it?

Talkback.

Survey: 37% of employees would become insiders given the right incentive | ZDNet

Would you sell sensitive company data if you're offered the right incentive? Using the current economic situation, or pure greed as an excuse, 37% of employees surveyed at this year's [Infosecurity Europe](#) event said that they are keeping their options open.

What type of information are they willing to sell, and [what kind of incentives are the potential insiders interested in?](#)

The surveyed employees had access to the following company assets:

- 83% had access to customer databases
- 72% has access to business plans
- 53% had access to accounting systems
- 51% had access to HR databases
- 31% had access to IT admin passwords

The incentives that they required in order to hand over sensitive data:

- 63% required at least 1 million pounds to convert to insiders
- 10% would become insiders if their mortgage was paid off
- 5% are willing to participate in exchange for a holiday
- Another 5% would do it if they are offered a new job
- 4% would participate if their credit card debt is covered

In respect to bribery, is it always about the right incentive, offered at the right moment in time if you're to take the quality of the survey results for granted? It's all a matter of perspective, but controversial to the emphasis of the survey, namely, that criminals are getting more interested in bribing your company's employees into committing insider acts, recent cases speak for the true self-serving mentality of insiders :

January, 2008 - [New Jersey system administrator gets 30 months in prison](#) for a logic bomb that he planted fearing potential layoffs
July, 2008 - [fearing potential layoffs](#) , network administrator working

for San Francisco's Department of Technology held the city hostage April, 2009 - apparently impatient to be recruited from potential criminals, a [system administrator attempts to extort his employer](#) after getting fired

April, 2009 - another impatient to be recruited [IT worker at the Federal Reserve Bank of New York](#) has been caught stealing personal customer data and obtaining loans in the process

The big also picture speaks for itself. According to [Verizon's 2009 Data Breach Investigations Report](#) , *74% of the data breaches resulted from external sources* (+1% increase from [2008](#)), with only *20% caused by insiders* (+2% increase from [2008](#)), followed by insecure practices on behalf of business partners.

Disgruntled employees are always going to be there, especially in today's [cloudy economic climate](#) . But a simple cost-effectiveness analysis performed by a criminal attempting to recruit your employees, would reveal that what he's trying to obtain may be much more easily, even cheaper to obtain through external means.

Study: US tops Zeus hosting infrastructure chart | ZDNet

According to a recently released study into the activities of the notorious Zeus crimeware, researchers from Trusteer sampled malicious activity from random Zeus botnets, to find out that the United States tops the C&C (command and control) hosting chart. Despite the clear U.S dominance, the main emphasis of the study is the slight increase in Eastern European hosting share compared to the U.S.

[More info:](#)

Our research shows that the US (39.8 per cent), Russia (21.6 per cent) and Ukraine (6.5 per cent) were the top three countries, with Eastern Europe accounting for 32.0 per cent of Zeus configs. That doesn't mean other countries are off the hook, as China, Malaysia, Iraq and Canada - along with Germany, the UK and the Netherlands in the EU territories - are also responsible for Web sites with hosted Zeus environments.

The analysis of sites IP accessible over the last 80 days makes for some interesting reading, as 29 per cent were found to be US Web sites, with Ukraine (17 per cent) and Russia (14 per cent) once again joining the US on the Zeus hall of shame podium.

[The Zeus tracker](#) , a free service tracking and sharing Zeus crimeware activity data, currently shows that Russia (73) is hosting more command and control servers than the United States (67). These minor fluctuations are pretty common, and speak for nothing else, but the dynamic nature of the hosting providers that cybercriminals use.

See also:

[Researchers peek inside a mini Zeus botnet, find 60GB of stolen data](#) [RSA: Banking trojan uses social network as command and control server](#) [Report: Zeus crimeware kit, malicious PDFs drive growth of cybercrime](#)

What's the connection between the fact that the U.S. is clearly dominating the hosting infrastructure, and the actual infection rates on a per country basis?

Cybercriminals always go where the higher purchasing power is. In fact, some of the affiliate networks that share revenue with the cybercriminals for successfully infecting a host, on purposely do not accept infections from Eastern European countries, namely, despite the fact that the hosts are infected, cybercriminals would rarely pay them any special attention, compared to hosts located in countries known to have a higher purchasing power online.

Study: Rootkits target pirated copies of Windows XP | ZDNet

During the six month study, researchers from Avast have sampled 630, 000 Windows rootkits, to find out that the majority [have infected pirated copies of Windows XP](#).

According to the study, 74% of infections originated from Windows XP machines, compared to 17% for Vista and only 12% from Windows 7 machines. The study also found that rootkits infecting via the MBR were responsible for over 62% all rootkit infections. Driver infections made up only 27% of the total. The clear leader in rootkit infection were the Alureon(TDL4/TDL3) family, responsible for 74% of infections.

With millions of PCs behind the WGA (Windows Genuine Advantage) wall, the number of infections is prone to increase. Not surprisingly, the researchers contribute the limited number of infections affecting Windows 7 to the availability of UAC, Patchguard and Driver Signing in the latest Windows versions.

Study: password resetting 'security questions' easily guessed | ZDNet

How secret are in fact the 'secret questions' used for resetting forgotten passwords? Not so secret after all, according to a just published study entitled "[It's no secret: Measuring the security and reliability of authentication via 'secret' questions](#) " according to which 17% of the study's participants were not only able to answer the 'secret questions' of strangers, but also, that the most popular questions were in fact the easiest ones to answer.

Here's an abstract from the study presented at this year's [IEEE Symposium on Security and Privacy](#) , by **Stuart Schechter** , **A. J. Bernheim Brush** , and **Serge Egelman** :

"We ran a user study to measure the reliability and security of the questions used by all four webmail providers. We asked participants to answer these questions and then asked their acquaintances to guess their answers. Acquaintances with whom participants reported being unwilling to share their webmail passwords were able to guess 17% of their answers. Participants forgot 20% of their own answers within six months. What's more, 13% of answers could be guessed within five attempts by guessing the most popular answers of other participants, though this weakness is partially attributable to the geographic homogeneity of our participant pool."

Moreover, upon assessing the memorability of the 'secret questions', the user study involving 130 participants (64 male and 66 female) also found out that the harder ones to guess were also the hardest ones to remember.

Two similar recently conducted studies confirm these findings. For instance, in "[Choosing Better Challenge Questions](#) " **Mike Just** and **David Aspinall** found out that users also tend to stick to low entropy answers which are potentially vulnerable to brute forcing attacks. The researchers came to the same conclusion in their second study "[Challenging Challenge Questions](#) " pointing out that given the average answer length of less than 8 characters, the authentication

system relying upon only a single security question is highly vulnerable to brute force attack.

And whereas brute forcing attempts against the security questions is a feasible attack tactic, malicious attacks tend to be a little bit more pragmatic than that, especially in a Web 2.0 world where the majority of their potential victims have already unconsciously/consciously published the answers to their security questions on the Web.

Case in point - the applicability of their findings can be confirmed through real-life incidents. For instance, [the Sarah Palin hacker managed to reset her password by Googling for the answer](#) to her 'secret question', followed by two similar [password resetting attacks aimed at Twitter employees](#) throughout the past one year. Moreover, a huge percentage of the commercial '[password recovery services](#) ' or email hacking for hire propositions rely on [password resetting attacks](#) next to the plain simple malware infection, and attempt to [exploit a XSS flaw within a particular web based email service provider](#) .

All of these findings, combined with the misalignment of the end user's perception of security offered by security questions and the extend to which the answers have already been made public, can be summarized with a single security tip - make sure that you don't tweet about how much fun you had on your honeymoon in Paris a couple of years ago, when your security question is "*Where did you spend your honeymoon?* ", which you would have presumably answered correctly.

What do you think, are security questions a viable form of authentication? Talkback.

Study: IE8's SmartScreen leads in malware protection | ZDNet

A recently released [NSS Labs study](#) , claims that Internet Explorer 8 greatly outperforms competing browsers in terms of protecting users [against web based malware](#) .

According to the study based upon a modest sample of 492 URLs, not only is IE8's [SmartScreen Filter](#) achieving a leading position against the rest of the popular browsers, but also, it also outperforms them in terms of the average time it takes to block known and already tested malicious sites. Among the key conclusions is that Opera 9.64 and Internet Explorer 7 provide "practically no protection against malware".

Here's how the study ranks the browsers:

Microsoft Internet Explorer v8 (RC1) achieved 69% block rate
Mozilla Firefox v3.07 achieved just over 30% block rate
Apple Safari v3 achieved 24% block rate
Google Chrome 1.0.154 achieved 16% block rate
Opera 9.64 achieved 5% block rate
Microsoft Internet Explorer v7 achieved 4% block rate

The study's methodology is however, greatly flawed at several key points, making its conclusions open to interpretation which should be the case when making such comparative tests.

Go through related posts detailing the growth of client-side vulnerabilities: [Secunia: popular security suites failing to block exploits](#) ; [Google introducing Safe Browsing diagnostic to help owners of compromised sites](#) ; [Report: 92% of critical Microsoft vulnerabilities mitigated by Least Privilege accounts](#)

For starters, NSS Labs undertook a rather minimalistic approach towards the definition of web malware. In this study, the malware URLs they're using are basically "*links that directly lead to a download that delivers a malicious payload* ", a decision that directly undermines the statement of "block rate" in times when client-side vulnerabilities are massively abused courtesy of web malware

exploitation kits. And since no live exploit URLs were taken into consideration, the [DEP/NX Memory Protection feature](#) within IE8 was naturally not benchmarked against known exploits-serving sites, or at least wasn't mentioned in the report.

Moreover, the [competing browsers'](#) use of SafeBrowsing's API, a combination of automatic (honey clients) and community-driven efforts to analyze a web site in a much broader "malicious" sense has a higher potential to maintain a more comprehensive database of known badware sites. It also comes as a surprise that Firefox, Safari and Chrome have such a varying block rates given that the browsers take advantage of the SafeBrowsing project's database. Basically, having a set of ten malicious URLs and running it against the browsers is supposed to return identical results due to the centralized database of known badware sites.

Interestingly, the study used Apple Safari v3 in order to come up with the 24% block rate, which excludes the built-in [anti-phishing and anti-malware features introduced in Safari v4](#) . The report is released prior to IE8's debut, but even if NSS's study is in fact relevant in a real-life attack scenario, does it really matter that IE8's outperforms the rest of the browsers in times when [IE8 users are downgrading to IE7](#) ? That very same IE7 which according to the study is offering "practically no protection against malware"?

Anyway, consider [going through the report](#) , with a salt shaker in hand.

Study finds the average price for renting a botnet | ZDNet

Based on an [experiment conducted by](#) researchers from [VeriSign's iDefense Intelligence Operations Team](#), involving 25 different "rent a botnet/DDoS for hire" underground marketplace propositions, they were able to conclude that the average price for renting a botnet is \$67 for 24 hours, and \$9 for hourly access.

With only two static things within the underground marketplace that I can think of right now - greed and potential for growth, personally, I think that static price lists for a particular service don't fall within this category.

Here's why.

The dynamics of the underground marketplace, have greatly matured throughout the past couple of years. The logical shift from static pricing lists, to the embracing of multiple pricing schemes such as [price discrimination](#) (differentiated pricing), or [penetration pricing](#), naturally resulted in different prices for different targeted groups.

Basically, the propositions analyzed by iDefense, can be best described as variables that are tailored to different customers.

For instance, starting from the basic fact that [cybercriminals actively multitask on multiple fronts](#), and the fact that access to botnets as an asset is a commodity good within the underground marketplace these days, certain propositions will even offer the "botnet for hire" option as a bonus/value-added service.

Moreover, what differentiates the sampled services from the hardcore IT underground ones, is the fact that the majority of these explicitly state that they reserve their right not to attack (any) government web sites, or engage in activities that will attract attention to their activities.

On the other hand, the hardcore "rent a botnet" services will not only charge larger sums of money, but may even ask for another

cybercriminal to vouch for the new customer in an attempt to limit curious researchers from finding out more about their infrastructure.

One of the most novel approaches for acquiring new clients I've seen in a while, is a weird combination consisting of direct DDoS extortion, followed by penalties for delayed response -- true mafia style that's for sure -- and the offering of 30% discount in case the victim wants to DDoS the competition once he pays the ransom.

Not only is the company in question a victim of DDoS extortion, but once it pays it's offered a 30% discount if it rents the service from the same extortionists, as well as a "protection" with the extortionists promising to turn down offers from the competitors wanting to attack the now "protected customer".

Surreal, but a fact. Here's [an excerpt from the actual DDoS extortion letter](#) :

"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us. The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

You will also receive several bonuses. 1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day. 2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them."

The long term trends regarding botnets for hire or DDoS for hire services, look pretty disturbing due to a simple fact - based on the never decreasing supply of malware infected hosts, no matter how low they price their services, they will always make a profit out of it, in between increasing the availability of such services to the general public.

From another perspective, this very same ["general public"](#) is slowly [starting to realize](#) that sometimes, [experience cannot be](#)

outsourced.

Image courtesy of a famous (in 2007), now taken offline botnet for hire service. Tip of the iceberg within the cybercrime ecosystem.

Stratfor subscribers targeted by passwords-stealing malicious emails | ZDNet

Cybercriminals are quick to capitalize on the Stratfor database leak, and are currently spamvertising malicious emails impersonating the company.

Researchers from Barracuda Labs have [intercepted a malicious email campaign impersonating the company](#). Using “*Stratfor: Beware of false communications*” subjects, the emails contain a PDF file enticing end and corporate users into downloading an antivirus package (supposedly McAfee).

Detected as PWS-Zbot.gen.ry, the bogus antivirus package will harvest stored passwords from the infected hosts and send them back to the command and control server. Moreover, the malware will scan the local hard drive for .PDF, .XLS and .DOC files, and will upload them to a remote site, relying on the File Transfer Protocol (FTP).

Users are advised to avoid interacting with the emails, and immediately report them as spam/malicious.

Storm Worm's Independence Day campaign | ZDNet

A Storm Worm's Independence Day campaign is circulating online using email as propagation vector, attempting to trick

users into visiting a Storm Worm infected host, where a multitude of what looks like over five different exploits attempt to automatically infect the visitors next to the malware binary **fireworks.exe**. Historically, Storm Worm is constantly changing its tactics, and the use of live exploit URLs is back in their arsenal for the last couple of campaigns. Therefore, visiting a Storm Worm infected IP sent to your email would launch multiple exploits against your third-party software. Here's a sample message used in the latest campaign :

"Colorful Independence Day events have already started throughout the country. The largest firework happens on the last weekday before the Fourth of July. Unprecedented sum of money was spent on this fabulous show. If you want to see the best Independence Day firework just click on the video and run it."

Storm Worm is [a case study on successful social engineering attacks](#) based on the timing, combination of tactics, and their persistence. In this particular campaign, they rely on the fact that a lot of users would be clicking on their exploit serving links from their homes, and that being away from the at least theoretically better hardened corporate network, would result in more infections. Storm is among the many other botnets currently active online, which when partitioned and access to them resold to different parties, make it harder to keep track of its size, since the wannabe botnet masters introduce new malware on the Storm Worm infected hosts, using them as foundation for creating their own unique botnet.

Moreover, the stereotype of zero day vulnerabilities as the critical success factor for a malware campaign, was originally broken by the time Storm Worm took the leading position as [the largest botnet online for a certain period of time](#), without exploiting a single zero

day vulnerability but relying on the fact that unpatched vulnerabilities are just as effective as zero day vulnerabilities when you diversity the exploits set well enough.

In times when client-side vulnerabilities are driving the success rates of malware campaigns, unpatched software or third-party software is just as vulnerable as unpatched software or third-party software that's getting exploited with a zero day vulnerability. So consider [self-auditing_yourself](#) by ensuring you're not running unpatched third-party software, and stay away from spam and phishing emails enticing you to visit a particular URL in general, since both are starting to converge with malware.

Storm Worm says the U.S have invaded Iran | ZDNet

Right after the [U.S Independence Day fireworks](#) , Storm Worm latest campaign launched a couple of hours ago, is

back online this time attempting to once again exploit client-side vulnerabilities, this time serving **iran_occupation.exe** by spreading false rumors of U.S invasion in Iran. The text reads :

"Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received today morning. Click on the video to see first minutes of the beginning of the World War III. God save us. "

Despite that you're highly advised to stay away from spam and phishing emails in general unless you know what you're doing, the latest Storm Worm domains used in the "Iran invasion campaign" should get a priority for the time being :

statenewsworld . com morenewsonline . com dailydotnews . com dotdailynews . com newsworldnow . com

'Steve Jobs Alive!' emails lead to exploits and malware | ZDNet

Cybercriminals are quick to capitalize on the death of Steve Jobs.

[Security researchers from M86 Labs](#) have intercepted a currently spreading malware campaign using Steve Jobs as a social engineering theme.

Sample subjects used in the campaign:

Steve Jobs Alive!; Steve Jobs Not Dead!; Steve Jobs: Not Dead Yet!; Is Steve Jobs Really Dead?

Upon clicking on the links the visitors are redirected to a obfuscated malware-serving page, courtesy of a [popular web malware exploitation kit](#) known as the BlackHole exploit kit. The exploit kit attempts to exploit popular [client-side vulnerabilities](#) in installed applications or [browser plugins](#).

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

SpyEye gets new DDoS functionality | ZDNet

Researchers from [RSA's FraudAction Research Lab are reporting](#) on a recently discovered new DDoS module within the popular crimeware SpyEye. Based on [various conversations within the cybercrime ecosystem](#) -- I also get a mention there -- the primary application of the plugin would be to attack legitimate sites such as Abuse.ch's [ZeusTracker](#), and the [SpyEye tracker](#), a community-driven services aiming to track crimeware campaigns.

The DDoS plugin currently offers SYN Flood; UDP Flood and Slowloris Flood, modes of operation.

Next to the new module, the researchers have also observed a new trend aiming to generate additional noise and poison the results offered by the two services. By including legitimate sites next to the malicious one, cybercriminals aim to make it harder for the service to distinguish between legitimate and purely malicious ones:

This means that all the credentials collected by the Trojan from SpyEye bots, including screenshots, username and password combinations, and stolen certificates and cookies, will be sent to port 443 of the legitimate websites, like the ones mentioned above. When abuse.ch's Trackers analyze SpyEye variants like the ones we traced, legitimate website domains will be classified as those variants' communication points. These, in turn, will show up in the SpyEye Tracker blocklist, and serve to diminish its credibility.

This isn't (See: [Crimeware tracking service hit by a DDoS attack](#)) the first coordinated attempt to disrupt the operation of the service, and definitely not the last, clearly speaking for its usefulness.

Spooky Halloween - scareware or crimeware? | ZDNet

With all the "spooky" cybercrime trends taking place on a monthly basis, such as [the death of CAPTCHA](#) , the suspicious idleness of the [Conficker botnet](#) , the clear presence of [government-tolerated](#) and upcoming [government-sponsored botnets](#) , the inevitable [migration from using malicious infrastructure](#) to entirely relying on [legitimate one](#) , followed by the cyber terrorism myopia that cyber terrorists still need years to build advanced cyber warfare capabilities, totally excluding outsourcing as a factor for gaining competitive advantage from the big picture, I'm literally having hard time deciding which one deserves most attention.

Whatever the cybercrime tactics, the main objective for the key 'market players' remains the same - monetization. Which prompts this year's Halloween question - [scareware](#) (trick) or [crimeware](#) (treat)?

The mentality of the average cybercriminal, or the ones managing the affiliate networks fueling the growth of the scareware business model is fairly simple - they're not trick-or-treaters, they're trick-AND-treaters. Basically, due to their clear multi-tasking, even if they manage to trick an average Internet user into purchasing their fake security software, they'll also attempt to compromise his E-banking account through another campaign managed by the same gang.

The [ongoing spam campaigns](#) serving [Zeus crimeware](#) , and active [blackhat search engine optimization campaigns managed by a high-profile gang](#) actively participating in the scareware business model, and the [Halloween-themed spam campaigns](#) , all indicate the efforts and clear multi-tasking which is a daily routine.

Scareware or crimeware for his Halloween? The end user and the enterprise network is equally exposed to both due to the cybercriminals' basic understanding of profit maximization.

Take control of the holiday - learn their tricks and avoid their treats.

Spoofed LinkedIn emails serving client-side exploits | ZDNet

Cybercriminals are currently brand-jacking LinkedIn in an attempt to trick end users into clicking on client-side exploits serving links found in the spoofed emails.

According to [security researchers from GFI Labs](#), the spamvertised campaign is redirecting users to the Black Hole web malware exploitation kit, that is ultimately dropping a Cridex malware variant on the infected PCs.

Spamvertised subjects

LinkedIn Invitation from your colleague
LinkedIn Invitation from your co-worker
LinkedIn Reminder from your colleague
LinkedIn Notification
LinkedIn private message

Spamvertised message:

There are a total of 1 messages awaiting your response. Visit your InBox now.

End and corporate users are advised to avoid interacting with the emails, and to ensure that they are running the [latest versions of their third-party software](#) and [browser plugins](#).

SpamZa - opt in spamming service fighting to remain online | ZDNet

A recently launched unethical spam list building service called SpamZa, is fighting to remain online after providing highly

successful ([87 spam emails in 8 minutes](#)) into fulfilling its objective, namely, to sign up any email submitted to hundreds of newsletters anonymously.

What is SpamZa anyway? SpamZa is a "creative" spammer's tactic for building spam lists containing legitimate emails, which will not only be spammed with the service owner earning revenue in the process, but will also get resold to other spammers. Despite that this is a spamming operation, their disclaimer is forwarding the responsibility to the end user helping them build the spam lists - *"SpamZa never send spam or unsolicited e-mails. You are solely responsible for the e-mail you choose to enter. SpamZa takes no responsibility in what you choose to submit."*

From *"Sign up any email without confirmation for free spam. SpamZa.com will sign up this email to hundreds of newsletters anonymously"* to *"SpamZa is currently down because some host has less balls than it said it did. We are currently actively looking for a new host. We WILL be back. We never give up."* Know a host that might be interested in hosting us? Drop us a line at admin@spamza.com. We will give a generous percentage of all advertising revenue. As an informative purpose only, our best day earnt us 35\$ -- and we are still very very small. Please contact us if you are ready to host SpamZa or if you have any question " the service is desperately trying to remain online.

Can they make it? Unless 1&1 Internet Inc. reacts to the fact that it's hosting the service for the time being, they could remain online for a little longer.

SpamZa's vision according to SpamZa itself is pretty self-descriptive on the real nature of the service :

"SpamZa.com is a website designed to promote newsletters and interesting content. WE DO NOT SEND SPAM.

SpamZa will subscribe the e-mail you submit to hundreds of popular and free newsletters. You can leave these newsletter at any time. Simply speaking, you put any e-mail, you click "Spam this email!" and we do the rest.

SpamZa was created with the idea that spam and newsletters were our friends, not our enemies. Think about it for a second: some people worked really really hard to write interesting newsletters and emails. The least we can do is read it! SpamZa will subscribe any email sent to hundreds and hundreds of newsletters. Furthermore, its algorithm always being under development, you can expect the e-mail owner to make a lot of friends from Nigeria who have a lot of money to give and he can expect to have your Bank of America/Citigroup/eBay/Paypal account suddenly locked with a poorly written email from LOLUGETSCAMMED@PHISINGROFLMAO.com. You know all the newsletters that say "we do not redistribute or resell your email" (but do anyway)? We do the opposite.

We get your email known, and pretty well known to as many newsletters are possible. Expect any email

entered in our form to receive 100-150 emails per day at the bare minimum, most being able to bypass most junk filters. To use our service, enter any email and click "Spam this email!" and get ready to get spammed. You may enter any email you want but please understand this is very, very mean to use. For maximal efficiency, enter the email every day and re-spam it, so even if the person unsubscribe, he'll get in again the next day.

SPAMZA DOES NOT SENDS SPAM. SPAMZA TAKES NO RESPONSABILITY FOR THE E-MAIL YOU CHOOSE TO SUBMIT TO OUR ALGORITHM. SPAMZA WAS CREATED TO PROMOTE POPULAR NEWSLETTERS AND NOT FOR SPAM. SpamZa is perfectly legal and respect all anti-spam policies around."

In reality, this "spam your enemies" model has proven highly successful during the years relying on nothing else but its social engineering appeal, with several other related services known to

have been developed in the past, perhaps among the main reasons why these intermediaries aren't yet going mainstream is because spammers, phishers are malware authors consolidated and are now exchanging more data and resources than never before, making the need for such services obsolete these days.

Spamvertised 'You have received a gift from one of our members!' malware campaign | ZDNet

[MXLab.eu is reporting](#) on a currently spamvertised malware campaign dropping Backdoor.IRCBot which, once executed, opens a connection back to an IRC (Internet Relay Chat) server, allowing the botnet masters easy of control.

Sample message:

Hello friend !You have just received a screensaver from someone who really cares about you!This is a part of the message:"Hi there! It has been a very long time since I haven't heard anything from you! I hope you enjoy this gift from me that i've sent with love ... I've just found out about this service from Sharon, a friend of mine who also told me that..."If you'd like to see the rest of the message click here to receive your 3d live Dolphins=====Thank you for using www.freeze.com 's services !!! Please take this opportunity to let your friends hear about us by sending them this screensaver from our personal collection !=====

From a social engineering perspective this is a -- thankfully -- badly executed campaign lacking basic quality assurance elements typical for social engineering campaigns such as timing -- see the Xmas photo -- which could have contributed to a better infection rate.

It seems though the the ubiquitous "You've received a screensaver" social engineering campaign is still favored by novice botnet masters.

Spamvertised Xerox document themed malware campaign spreading | ZDNet

A currently [spamvertised malware campaign](#) attempts to trick the user into thinking he's received a scanned Xerox document, whereas the actual attachment is a malicious PDF file, which once successfully exploiting the CVE-2007-5659; CVE-2008-2992; CVE-2009-0927 and CVE-2009-4324 flaws drops scareware on the infected host.

Sample message:

Hello, It was scanned and sent to you using a Xerox WorkCentre Pro. Please open the attached document.

Sent by: Guest Number of images: 1 Attachment File type: PDF.
WorkCentre Pro Location: Machine location not set

Device name: XERX911818091004676018486

Attachment name: 02-02-2011-43.pdf

As far as the social engineering theme is concerned, [cybercriminals periodically reintroduce and rotate it](#) once the campaign receives the necessary media coverage.

Users are advised to go through the [Ultimate Guide to Scareware Protection](#) , and ensure their hosts are client-side vulnerabilities free with [Secunia's Personal Software Inspector \(PSI\)](#) .

Spamvertised 'We are going to sue you' emails lead to malware | ZDNet

Security researchers from WebSense have intercepted a currently [active and circulating malicious spam campaign](#).

The spamvertised emails contain subjects and messages attempting to socially engineer users into thinking that spam is coming from their mailboxes, and that they face legal action:

In this campaign, emails are spoofed to appear as though they are sent from established companies. The emails even formally claims that legal action will be taken because of the spam you have sent. These emails with the fake warning even attach a ZIP file that contains a scanned copy of a document that is supposed evidence of your spam.

[-Spamvertised subjects include :](#)

We will be impelled to sue you
We are going to sue you
We are suing you
You are sending add messages
A message from our security service

[- Spamvertised body of the message:](#)

Hello. Your email is sending spam messages. If you don't stop sending spam, we will be impelled to sue you! We've attached a scanned copy of the document assembled by our security service to this letter. Please care carefully read through the document and stop sending spam messages. This is the final warning.

[-Detection rate](#) for the [spamvertised malware](#).

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Related posts:

[Spamvertised 'Scan from a Xerox WorkCentre Pro' leads to malware](#) [Malware Watch: FDIC and Western Union themed emails lead to malware](#) [Spamvertised 'Facebook notification' leads to](#)

exploits and malware Spamvertised Uniform traffic tickets and invoices lead to malware Spamvertised United Parcel Service notifications lead to malware Spamvertised United Parcel Service emails lead to scareware Federal Reserve themed emails lead to Zeus crimeware 'McDonald's Free Dinner Day' emails lead to scareware Spamvertised bank statements serving scareware Spamvertised Post Office Express Mail (USPS) emails lead to malware Spamvertised "Reget Rejected" campaign leads to scareware Spamvertised 'Facebook. Your password has been changed!' emails lead to malware

Spamvertised United Parcel Service notifications lead to malware | ZDNet

A currently spamvertised campaign is brand-jacking United Parcel Service (UPS) for malware-serving purposes.

Sample subject: United Parcel Service notification

Sample attachments: [UPSnotify.rar](#); [UPSnotify.exe](#)

Sample message: *Dear customer. The parcel was sent your home address. And it will arrive within 7 business day. More information and the tracking number are attached in document below. Thank you. © 1994-2011 United Parcel Service of America, Inc.*

Upon execution the malware (**UPSnotify.exe**) downloads additional binaries including a scareware variant. Users are advised to avoid interacting with suspicious attachments.

Spamvertised United Parcel Service emails lead to scareware | ZDNet

A currently ongoing [malware campaign](#) is impersonating the United Parcel Service (UPS) in an attempt to trick users into executing the malicious UPS_Document.zip attachment.

Sample attachments: *UPS_Document.zip*

Sample subject: *United Parcel Service notification*

Sample message: *Good morning Parcel notification, The parcel was sent your home adress. And it will arrive within 3 buisness days. More information and the parcel tracking number are attached in document below. Thank you*

United Parcel Service of America (c) 153 James Street, Suite100, Long Beach CA, 90000

Upon execution the malware sample downloads scareware variant detected as Mal/FakeAV-LI. Users are advised to pay extra attention when interacting with suspicious emails.

Related posts:

[Spamvertised United Parcel Service notifications lead to malware](#)
[Spamvertised Post Office Express Mail \(USPS\) emails lead to malware](#)
[Spamvertised "Reget Rejected" campaign leads to scareware](#)
[Spamvertised 'Facebook. Your password has been changed!' emails lead to malware](#)

Spamvertised Uniform traffic tickets and invoices lead to malware | ZDNet

Researchers from Sophos have intercepted two currently active [spamvertised malware campaigns](#), enticing users into downloading and [executing malicious attachments](#).

The first campaign is attempting to trick users into thinking that they have received a uniform traffic ticket, and are charged with speeding at 7:25 AM on the 5th July 2011. The malicious attachment **Ticket-O64-211.zip** is currently detected as Mal/ChepVil-A.

The second campaign is relying on inter-company invoices impersonating Beazer Homes, KPMG, Miltek, Kraft Foods, and Safeco. The spamvertised **Inv._08.8_D7.zip**, **Corpinvoice_08.10_N47.zip**, and **Invoice_08.4_D6.zip** are currently detected as Troj/Agent-TBO.

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Related posts:

[Spamvertised United Parcel Service notifications lead to malware](#)
[Spamvertised United Parcel Service emails lead to scareware](#)
[Federal Reserve themed emails lead to Zeus crimeware](#)
['McDonald's Free Dinner Day' emails lead to scareware](#)
[Spamvertised bank statements serving scareware](#)
[Spamvertised Post Office Express Mail \(USPS\) emails lead to malware](#)
[Spamvertised "Regest Rejected" campaign leads to scareware](#)
[Spamvertised 'Facebook. Your password has been changed!' emails lead to malware](#)

Spamvertised 'Tax information needed urgently' emails lead to malware | ZDNet

Security researchers from AppRiver, have intercepted a [currently spamvertised malware campaign](#), enticing end users into clicking on malicious links.

Impersonating INTUIT Inc., the maker of the popular tax software TurboFax, cybercriminals are spamvertising links are attempting to trick end users into thinking that *"it appears that your name and/or Taxpayer Identification Number, that is stated on your account is different from the data obtained from the Social Security Administration "*, and that by clicking on link found in the malicious email, they will get the opportunity to check the data on their account.

Upon clicking on the link, a trojan horse is dropped on the targeted PC using a malicious Javascript.

Users are advised to avoid interacting with suspicious emails, and to ensure that their hosts are free from vulnerabilities most commonly exploited by web malware exploitation kits.

Spamvertised 'Scan from a Xerox WorkCentre Pro' leads to malware | ZDNet

Researchers from Sophos have [intercepted a currently circulating malware campaign](#), enticing users into downloading and executing malicious file attachments.

The campaign attempts to trick users into thinking that they have received an email from a Xerox WorkCentre Pro photocopier, and has the following filenames attached to it
Xerox_Document_08.23_C11125.zip ;
Xerox_Scan_08.23_K1274.zip .

Spamvertised as:

Please open the attached document. It was scanned and sent to you using a Xerox WorkCentre Pro.Sent by: GuestNumber of Images: 1Attachment File Type: ZIP [DOC]WorkCentre Pro Location: machine location not setDevice Name: [random]

Related posts:

[Spamvertised Uniform traffic tickets and invoices lead to malware](#)
[Spamvertised United Parcel Service notifications lead to malware](#)
[Spamvertised United Parcel Service emails lead to scareware](#)
[Federal Reserve themed emails lead to Zeus crimeware](#)
['McDonald's Free Dinner Day' emails lead to scareware](#)
[Spamvertised bank statements serving scareware](#)
[Spamvertised Post Office Express Mail \(USPS\) emails lead to malware](#)
[Spamvertised "Reget Rejected" campaign leads to scareware](#)
[Spamvertised 'Facebook. Your password has been changed!' emails lead to malware](#)

Users are advised not to interact with suspicious emails, or [spam emails](#) in general.

Spamvertised 'Scan from a HP OfficeJet' emails lead to exploits and malware | ZDNet

Security researchers from Sophos have intercepted [a currently spamvertised malware campaign](#), enticing end and corporate users into downloading and viewing a malicious HTML file.

Sample subjects include:

Re: Fwd: Scan from a Hewlett-Packard Officejet 69087080
Fwd: Re: Scan from a HP Officejet #43384897
Fwd: Re: Scan from a Hewlett-Packard Officejet #1584730
Re: Scan from a Hewlett-Packard Officejet 1206754
Re: Fwd: Fwd: Scan from a Hewlett-Packard Officejet #886303 1.2
Re: Fwd: Fwd: Scan from a HP Officejet #75709542
Fwd: Re: Fwd: Scan from a Hewlett-Packard Officejet #128469
Fwd: Re: Re: Scan from a Hewlett-Packard Officejet #662447
Re: Scan from a HP Officejet #49477094
Fwd: Fwd: Scan from a Hewlett-Packard Officejet #885932
Fwd: Fwd: Scan from a HP Officejet #09665907

Once the end user downloads and previews the malicious attachment, a script inside the HTML file will attempt to load client-side exploits for external compromised web sites.

End and corporate users are advised to report the emails as spam/malicious and avoid interacting with the content of the email messages.

Spamvertised "Requet Rejected" campaign leads to scareware | ZDNet

A currently spamertised malware campaign is enticing end users into downloading and executing a malicious attachment.

Sample subject: Requet rejected **Sample message:** *"Dear Sirs, Thank you for your letter! Unfortunately we can not confirm your request! More information attached in document below. Thank you Best regards. "* **Sample attachments:** EX-38463.pdf.zip; EX-38463.pdf.exe

Upon execution the binary downloads additional files, in this case a scareware variant. Detection rate for [TrojanDownloader:Win32/Chepvil.J](#).

See also:

[Spamvertised Post Office Express Mail \(USPS\) emails lead to malware](#) [Spamvertised DHL notifications lead to malware](#) [The Ultimate Guide to Scareware Protection](#)